The right to privacy: How the proposed POPI Bill will impact data security in a Cloud Computing environment

By

Benhardus Basson

Thesis presented in partial fulfilment of the requirements for the degree Masters of Commerce (Computer Auditing) at Stellenbosch University

Supervisor: Ms. Anria Van Zyl

! LJNXf 201n

Declaration

I, the undersigned, hereby declare that the work contained in this assignment is my own original work and that I have not previously submitted it, in its entirety or in part, at any university for a degree.

_____

Benhardus Basson
November 2013

Abstract

The growing popularity and continuing development of cloud computing services is ever evolving and is slowly being integrated into our daily lives through our interactions with electronic devices. Cloud Computing has been heralded as the solution for enterprises to reduce information technology infrastructure cost by buying cloud services as a utility. While this premise is generally correct, in certain industries for example banking, the sensitive nature of the information submitted to the cloud for storage or processing places information security responsibilities on the party using the cloud services as well as the party providing them. Problems associated with cloud computing are loss of control, lack of trust between the contracting parties in the cloud relationship (customer and cloud service provider) and segregating data securely in the virtual environment.

The risk and responsibilities associated with data loss was previously mainly reputational in nature but with the promulgation and signing by the South African Parliament of the Protection of Personal Information Bill (POPI) in August 2013 these responsibilities to protect information are in the process to be legislated in South Africa. The impact of the new legislation on the cloud computing environment needs to be investigated as the requirements imposed by the Bill might render the use of cloud computing in regard to sensitive data nonviable without replacing some of the IT infrastructure cost benefits that cloud computing allows with increased data security costs.

In order to investigate the impact of the new POPI legislation on cloud computing, the components and characteristics of the cloud will be studied and differentiated from other forms of computing.
The characteristics of cloud computing are the unique identifiers that differentiate it from Grid and Cluster computing. The component study is focused on the service and deployment models that can be associated with cloud computing. The understanding obtained will be used to compile a new definition of cloud computing. By utilizing the cloud definition of what components and processes constitute cloud computing the different types of data security processes and technical security measures can be implemented are studied. This will include information management and governance policies as well as technical security measures such as encryption and virtualisation security. The last part of the study will be focussed on the Bill and the legislated requirements and how these can be complied with using the security processes identified in the rest of the study.

The new legislation still has to be signed by the State President after which businesses will have one year to comply and due to the short grace period businesses need to align their business practices with the proposed requirements. The impact is wide ranging from implementing technical information security processes to possible re-drafting of service level agreements with business partners that share sensitive information. The study will highlight the major areas where the Bill will impact businesses as well as identifying possible solutions that could be implemented by cloud computing users when storing or processing data in the cloud.

Uitreksel

Die groei in gewildheid en die ontwikkeling van wolkbewerking dienste is besig om te verander en is stadig besig om in ons daaglikse lewens geintegreer te word deur ons interaksie met elektroniese toestelle. Wolkbewerking word voorgehou as ‘n oplossing vir besighede om hul inligtings tegnologie infrastruktuur kostes te verminder deur dienste te koop soos hulle dit benodig. Alhoewel die stelling algemeen as korrek aanvaar word, kan spesifieke industrië soos byvoorbeeld die bankwese se inligting so sensitief wees dat om die inligting aan wolkbewerking bloot te stel vir berging en prosesseering dat addisionele verantwoodelikhede geplaas op die verantwoordelike partye wat die wolk dienste gebruik sowel as die persone wat dit voorsien. Probleme geassosieër met wolk-bewerking is die verlies aan beheer, gebrekkige vertroue tussen kontakteurende partye in die wolk verhouding (verbruiker en wolk dienste verskaffer) en die beveiliging van verdeelde inligting in die virtuele omgewing.

Die risiko’s en verantwoordelikhede geassosieër met inligtings verlies was voorheen grootliks gebasseer op die skade wat aan die besigheid se reputasie aangedoen kan word, maar met die publiseering en ondertekening deur die Suid-Afrikaans Parliament van die Beskerming van Persoonlike Inligting Wet (BVPI) in Augustus 2013 is hierdie verantwoordelikhede in die proses om in wetgewing in Suid Afrika vas gelê te word. Die impak van die nuwe wetgewing op die wolkbewering omgewing moet ondersoek word omdat die vereistes van die Wet die gebruik van wolkbewerking in terme van sensitiewe inligting so kan beinvloed dat dit nie die moeite werd kan wees om te gebruik nie, en veroorsaak dat addisionele verminderde IT infrastruktuur koste voordele vervang moet word met addisionele inligting beveiligings kostes.

Om die impak van die nuwe BVPI wetgewing op wolkbewerking te ondersoek moet die komponente en karakter eienskappe van die wolk ondersoek word om vas te stel wat dit uniek maak van ander tipes rekenaar bewerking. Die karakter eienskappe van wolkbewerking is die unieke aspekte wat dit apart identifiseer van Rooster en Groep rekenaar bewerking. Die komponente studie sal fokus op die dienste en implimenterings modelle wat geassosieer word met wolkbewerking. Die verstandhouding wat deur voorsafgaande studie verkry is sal dan gebruik word om ‘n nuwe definisie vir wolkbewerking op te stel. Deur nou van die definisie gebruik te maak kan die inligtings sekuriteit prosesse en tegniese sekuriteits maatreëls wat deur die verantwoordelike party en die wolkbewerkings dienste verskaffer gebruik kan word om die komponente en prosesse te beveilig bestudeer word. Die studie sal insluit, inligtings bestuur prosesse en korporatiewe bestuur asook tegniese beveiligings maatreels soos kodering en virtualisasie sekuriteit. Die laaste deel van die studie sal fokus op die BVPI wetgewing en die vereistes en hoe om daaraan te voldoen deur die sekuritiets maatreëls geidentifiseer in die res van die studie te implimenteer.

Die nuwe wetgewing moet nog deur die Staats President onderteken word waarna besighede ‘n jaar sal he om aan die vereistes te voldoen en omdat die periode so kort is moet besighede hulself voorberei en besigheid prosesse aanpas. Die impak van die wetgewing strek baie wyd en beinvloed van tegnise inligtings beveiligings prosesse tot kontrakte aangaande diens lewering wat dalk oor opgestel moet word tussen partye wat sensitiewe inligting uitruil. Die studie sal die prominente areas van impak uitlig asook die moontlike oplossings wat gebruik kan word deur partye wat wolkbewerking gebruik om inligting te stoor of te bewerk.

Acknowledgement

I would like to express my sincere gratitude the God that has blessed me in completing this assignment as well as my supporting family for the sacrifices that had to be made.

Table of Contents

List of Tables and Figures

Tables

Figures

Glossary of abbreviations

CSP – Cloud Service Provider

DDOS – Distributed Denial of Service attacks

DES – Data Encryption Standard

HTTP – Hypertext Transfer Protocol

HTTPS - Hypertext Transfer Protocol Secure

IDS – Intrusion Detection System

OS – Operating system

QoS – Quality of Service

RP – Responsible Party

SLA – Service level agreement

SQL – Structured Query Language

TC – Trusted Computing

TPM - Trusted Platform Module

VM – Virtual Machine

VMM – Virtual Machine Manager

Chapter 1 – Introduction and Methodology

1.1) Background

Cloud Computing is not an entirely new concept and the dream of computing as a utility has been around since 1961 when computing pioneer, John McCarthy predicted that "computation may someday be organised as a public utility"(J. McCarthy cited in Garfinkel, 2011). The "cloud" and the different names and formats it has been marketed as since then is ever evolving and the interaction with everyday life through interaction with electronic devices is becoming more common.

Cloud computing offers numerous benefits as well as some new unique hardware aspects such as the illusion of infinite up-front resources available on demand, the elimination of an up-front capital commitment by cloud users and the ability to pay for use of computing resources on a short-term basis as needed (Armbrust *et al.*, 2009).

Cloud computing thus realises the dream of selling computing as a utility and allows cloud computing providers the opportunity to build large data centres at a low cost and by managing and provisioning the processing and storage requirement cost savings can be achieved. The centralised management of resources allows for better utilisation and limits any costs associated with over capacity in a network (Chen & Paxson, 2010).

Cloud computing in this context refers to both the applications delivered as services over the Internet and the hardware and system software in the datacentres that provide those services (Armbrust *et al.*, 2009).

1.2) Purpose of the Study

"Cloud Computing is an emerging computing paradigm in which resources of the computing infrastructure are provided as services over the Internet" (Yu *et al.*, 2010). The description of what does and does not constitute cloud computing is wide ranging and in order to investigate the cloud security implications it has to be properly defined and isolated to allow exclusion of non-cloud based infrastructure and security processes.

This study investigates which technology forms part of the cloud environment by defining cloud computing, how to secure the cloud from a cloud service provider view as well as what a cloud customer has to be cognisant of when making the decision to use cloud computing.

The paper concludes with a review of the potential impact of the proposed Protection of Public Information Bill on the parties involved in the value chain of cloud computing.

1.3) Limitations of study

The study proposes to investigate whether the new Protection of Personal Information Bill will impact so negatively on the technical data security requirements of "Responsible parties" and "Cloud Service Providers" that it will negate some of the perceived benefits of cloud computing.

The impact of the Protection of Personal Information Bill when enacted on "cloud service providers" and "responsible parties" (data gatherers) is still unclear and has potentially far reaching implications for both parties. The study will investigate and discuss the impact based on available literature regarding technical data security in a cloud environment and the requirements of the Bill as proposed.

In order to investigate the impact on the cloud service providers and responsible parties clarity must first be obtained as to which outsourced services would constitute "Cloud Computing". To this end "Cloud Computing" will be defined in Chapter 2.

In Chapter 3 the security risks and technical security measures used to secure the cloud and data transfers will be investigated. This investigation is limited to the broad security measures available in the cloud computing environment. The list is not extensive or complete as there are numerous measures that can be used to secure networks, but a complete list is beyond the scope of this study. The measures identified will first be discussed on a technical basis and then in relation to how it can secure a cloud computing environment.

In Chapter 4 the requirements that the Bill imposes on cloud participants (The responsible party and operator as defined) will be investigated and linked back to the security control and measures that where identified in Chapter 3.

The research project is subject to the following limitations:

- Due to the fact that the Bill has still to be enacted and applicable case law and legal pronouncements and interpretations will only be made following the Bill's enactment by Parliament no legal interpretations will be investigated except those published as guidelines by the South African Law Society and other professional bodies.
- The Bill's sections will be interpreted in its simplest form and the focus of the study will be on the technical cloud and data security implications and how to address these.

1.4) Research Study methodology

Methodology steps:

Step 1: Define Cloud computing.

1. Perform a literature review of published journal articles and white papers relating to the following terms: Cloud computing, SAAS (Software as a Service), Private Cloud, Public Cloud, PAAS (Platform as a Service)
2. Define Cloud computing taking the readings in number 1 above into account.

Step 2: Investigate the data security frameworks and data security risks and controls in a cloud environment

1. List and discuss the risks associated with Cloud computing focusing primarily on those risks that impact on information security and privacy.
2. Investigate the data security frameworks and data security relevant to "cloud computing" and discuss this in terms of strategic risks and operational risk and the impact it has on mitigation of these risks.
3. Investigate the technical data security implications on cloud computing environment that might be impacted by the requirements of the POPI Bill.

Step 3: Form an understanding of the potential impacts of the Protection of Personal Information Bill.

1. Study the proposed Protection of Personal Information Bill in the format presented by the Portfolio Committee on Justice and Constitutional Development to the National Assembly and passed on 11 September 2012.
2. Investigate the impact of the proposed POPI legislation on cloud computing extending the research to both “responsible parties” and cloud computing providers (“operators”) in terms of the Bill.

Chapter 5 concludes the study with final remarks and findings as well as possible recommendations for future research.

Chapter 2 – Defining Cloud Computing

2.1) Introduction to defining cloud computing

A review of the available definitions and characteristics of cloud computing in available academic literature as well as other sources on the internet has indicated that the term is neither understood nor have the boundaries been defined as to what is included and excluded from the concept. Considerable uncertainty exists among consumers regarding what cloud computing is and which services can be classified as cloud services (Enslin, 2012). Cloud computing are current loosely defined, and such associated activities as photo sharing, social media, mobile phones, computers and servers are included in what consumers interpret as the cloud.

There are still no widely accepted definition for cloud computing albeit the cloud computing practice has attracted much attention.

Wang & von Laszewski (2008) identified the main reasons for the confusion as follows:

• Cloud computing information technology engineers and researchers approach cloud computing from different backgrounds and points of view. Based on their experience and points of reference they might view, for example grid computing, as a form of cloud computing.
• The technologies which are enablers of cloud computing such as Web 2.0 and Service Oriented Computing (SOC) are still evolving and progressing and the boundaries has not been clearly defined of what cloud computing constitutes.
• The limited use and uptake by businesses of existing computing clouds still lack large scale deployment and usage, which would finally justify the concept of cloud computing.

This study proposes to use the available definitions to identify the common thread that defines cloud computing as unique. This will require that the characteristics of cloud computing is investigated as a “new” definition can only be developed by identifying what types of processing is excluded form cloud computing.

The process to define cloud computing is that of elimination, firstly of concepts that are similar but have distinct differentiating characteristics and secondly to identify a definition by identifying cloud definitions and aggregating their commonalities.

2.2) Analysis of cloud computing commonalities

By first defining Clusters and Grids the commonalities with cloud computing can be identified and factors that are not part of the cloud computing environment can be excluded.

2.2.1) Definition of Clusters and Grids

Buyya, Yeo, Venugopal, Broberg, & Brandic (2008), define both Clusters and Grids as:

Cluster: ”A cluster is a type of parallel and distributed system, which consists of a collection of inter-connected stand-alone computers working together as a single integrated computing resource”.

Grid: "A Grid is a type of parallel and distributed system that enables the sharing, selection, and aggregation of geographically distributed 'autonomous' resources dynamically at runtime depending on their availability, capability, performance, cost, and users' quality of service requirements".

By keeping these definitions in mind a review of the unique characteristics of the cloud computing environment can be performed which will indicate the differences between the cloud and cluster computing and grid computing.

To investigate the building blocks of the cloud paradigm the US National Institute of Standards and Technology (NIST) definition will be used. (Mell & Grance 2011)

The definition provides the characteristics, deployment and service models that can be typically found in the cloud environment and by investigating each area the differences between the cloud and cluster and grid computing will be identified.

The second area to investigate is the unique characteristics of cloud computing.

2.2.2) Characteristics of Cloud Computing

The Characteristics of cloud computing are those unique identifying attributes that distinguishes cloud computing from any other distributed computing concept.

Table 2.1 – Cloud Computing Characteristics

CHARACTERISTIC	DESCRIPTION
On-demand self-service	A consumer can unilaterally request computing capabilities, such as server time and network storage, as needed automatically without requiring human interaction with each service's provider. Self-service cloud offerings must provide easy-to-use, intuitive user interfaces that equip users and empower them to be able to productively manage the service delivery lifecycle. Best of breed self-service provides users the ability to upload, build, deploy, schedule, manage, and report on their business services on demand.
Broad Network Access	Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms (e.g. Mobile phones, laptops, and PDAs).
Resource pooling	The provider's computing resources are pooled to serve multiple consumers using a

CHARACTERISTIC	DESCRIPTION
	multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand. There is a sense of location independence in that the customer generally has no control or knowledge over the exact location of the provided resources but may be able to specify location at a higher level of abstraction (e.g., country, state, or data centre). Examples of resources include storage, processing, memory, network bandwidth, and virtual machines.
Rapid Elasticity/ Dynamic infrastructure	Capabilities can be rapidly and elastically provisioned, in some cases automatically, to quickly scale out, and rapidly released to quickly scale in. To the consumer, the capabilities available for provisioning often appear to be unlimited and can be purchased in any quantity at any time. Cloud computer service providers need to invest in dynamic virtualized and standardised infrastructure. This enables expansion without requiring architecture rework.
Measured Service	Cloud systems automatically control and optimize resource use by leveraging a metering capability at some level of abstraction appropriate to the type of service (e.g. storage, processing, bandwidth, and active user accounts). Resource usage can be monitored, controlled, and reported, providing transparency for both the provider and consumer of the utilized service. Any Cloud computing service provider must provide mechanisms to capture usage information that enables chargeback reporting and/or integration with billing systems. This enables the user to monitor and control costs. Different models may be used for billing such as: Fixed tariff plans, Pay-as-u-use, Prepaid

Source: Adapted from (Mell & Grance 2011)

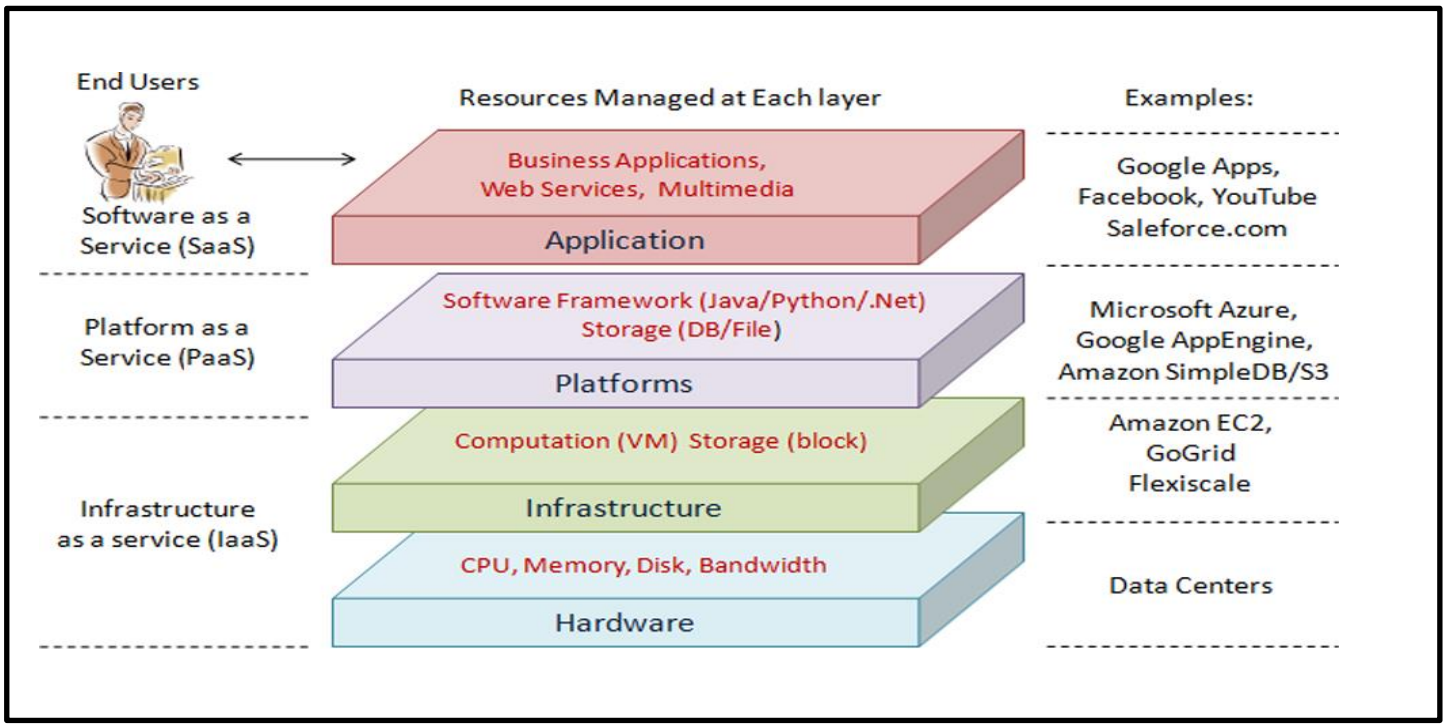
These attributes differentiates cloud computing form other forms of distributed computing and by extending the study to the service models employed in the cloud environment additional unique identifiers can be identified.

2.3) Service Models

The Service model to which a cloud conforms dictates an organisations scope and control over computational environment, and characterizes a level of abstraction for its use (Mell & Grace, 2011).

The most effective method to investigate and understand the service models applicable to cloud computing is to depict it graphically.

Figure 2.1 – Cloud Computing Architecture



Source: Zhang, Cheng & Boutaba (2010)

2.2.1) Cloud Software as a Service (SaaS)

The capability provided to the customer is to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through a thin client interface such as a web browser (e.g., web-based email). The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific applications configuration settings (Mell & Grace, 2011).

2.2.2) Cloud Platform as a Service (PaaS)

The capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created using programming languages and tools supported by the provider. The consumer does not manage or control the

underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly application hosting environment configurations (Mell & Grace, 2011).

2.2.3) Cloud Infrastructure as a Service (Iaas)

The capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, deployed applications, and possibly limited control of selected networking components (e.g., host firewalls) (Mell & Grace, 2011).

The layered architecture of the cloud is evident by the study of the service models and due to the interdependent nature of each layer on another they security in each layer impacts on the total security of the cloud. This interdependency will be further investigated in Chapter 3.

Cloud computing can be deployed in different models broadly characterized by the management and disposition of the computational resources for delivery of the cloud services to the end users (Jansen & Grance, 2011). Below these deployment models will be discussed further to assist in the identification of the unique characteristics of cloud computing.

2.4) Deployment Models

Cloud computing can broadly be distinguished by two distinct deployment models namely public cloud computing (or public cloud) or private cloud computing (or private cloud) as per Plummer *et al*. (2009).

Information Systems Audit and Control Association (2009) has expanded the deployment models into two additional distinct models namely a Community Cloud and a Hybrid Cloud.

Table 2.2 expands our understanding of these models.

Table 2.2 – Cloud Computing Deployment Models

DEPLOYMENT MODEL	CHARACTERISTICS
Private Cloud	• The cloud is operated soles for an organisation. • Managed by either the organisation or a third party. • Hosting could be onsite or at another location.
Community Cloud	• The cloud is shared by a number of organisations. • The organisations sharing the cloud have shared needs/requirements. • Examples of these shared needs are: security, policy and compliance. • The cloud can be managed by either the organisation or a third party. • Hosting could be onsite or at another location.
Public Cloud	• Cloud services made available to the general public

DEPLOYMENT MODEL	CHARACTERISTICS
	or large industry groups. • The Cloud Services are owned by a business selling cloud services.
Hybrid Cloud	• The Cloud infrastructure is a combination/ composition of two of the other cloud computing deployment models. • The two clouds remain unique entities. • Clouds are bound together by using standard or proprietary technology that enables data and application portability between clouds.

Source: Mell & Grance (2011) and Armbrust *et al*. (2009)

The investigation into the unique characteristics can now be supported with the available cloud computing definitions and by combining all of these factors and characteristics a new and complete definition can be compiled.

2.5) Literature study of existing cloud definitions

Available cloud computing definitions:

1) "A large-scale distributed computing paradigm that is driven by economies of scale, in which a pool of abstracted virtualised, dynamically-scalable, managed computing power, storage, platforms and services are delivered on demand to external customers over the Internet"(Foster, Zhao, Raicu, Lu, 2008).

2) A Cloud is a type of parallel and distributed system consisting of a collection of inter-connected and virtualised computers that are dynamically provisioned and presented as one or more unified computing resource(s) based on service-level agreements established through negotiation between the service provider and consumers (Buyya *et al.*, 2008).

3) Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction (Mell & Grance, 2011).

4) A Computing Cloud is a set of network enabled services, providing scalable, QoS guaranteed, normally personalized, inexpensive computing platforms on demand, which could be accessed in a simple and pervasive way (Wang & von Laszewski, 2008).

5) The main idea of cloud computing is to build a virtualized computing resource pool by centralizing abundant computing resources connected with network and present the service of infrastructure, platform and software (Che, Duan, Zhang & Fan, 2011).

6) Gartner defines **cloud computing** as a style of computing in which scalable and elastic IT-enabled capabilities are delivered as a service to external customers using Internet technologies (Gartner IT Glossary).

7) Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (for example, networks, servers, storage, applications and services) that can be rapidly provisioned and released with minimal effort or service provider interaction (Pallis, 2010).

As can be seen in the literature study of available cloud definitions there are varying interpretations of what cloud computing involves and how to define the paradigm.

Both Foster *et al*. (2008) and Vaquero, Rodero-Meniro, Caceres & Lindner, (2009) identify some unique characteristics that differentiate cloud computing from grid and cluster computing. The first concept is that of delivering services opposed to components. Secondly is the concept of payment based on usage and not on physical assets. Thirdly is the idea of scalability which includes the concepts of flexibility and low barriers to entry for customers. Finally the delivery of Internet Technologies implies that specific standards are adhered to and that multiple customers, leveraging shared resources increase the clouds economies of scale.

Using these unique characteristics a new cloud definition is compiled.

2.6) New Definition of Cloud Computing

Cloud computing is an on demand service based methodology of computing via the internet where hardware is shared by multiple users which is characterised by being scalable and flexible with low barriers of entry. The model is based on the fact that services are sold resulting in lower costs due to economies of scale. Users of cloud computing technology do not have to be technology experts and use of the technology is fairly uncomplicated.

The unique identifying characteristics highlighted above such as scalability and flexibility and low barriers to entry in the new definition sets cloud computing apart from the “supercomputers” of the past. Cloud computing enables users to acquire processing power and an almost infinite capacity to store data, additionally users only pay for the services and capacity used. Grid and cluster computing had a limited use in business life as it just was not accessible to businesses without large IT infrastructure expenses, but cloud computing has addressed the cost constraint and made processing power more accessible and cost effective.

With a better understanding of what constitutes the cloud computing paradigm the technology to secure the cloud can be investigated.

Chapter 3 – List and discussion of information security risks in a Cloud Computing environment and Technical solutions to limit these risks

3.1) Introduction

One of the major concerns associated with cloud computing is regarding security and trust between cloud computing parties (Bose, Luo, Lui, 2013). In order for cloud computing to become a viable option for businesses, in regard to the processing of sensitive information, the associated security processes will have to be enhanced to provide cloud clients with assurance regarding sensitive data. In order for cloud computing to grow in popularity these security risks will have be addressed and mitigated to an acceptable level.

The cloud computing environment has benefits such as scalability, flexibility and low barriers to entry that all result in lower IT infrastructure costs. These benefits are however only applicable if the data storage and processing that is performed in the cloud environment is secure and trusted by the customers of the cloud providers. This fear by customers of security in the cloud environment is reflected in a recent study of more than 500 chief executives an IT managers in 17 countries that resulted in the following findings that despite the potential benefits, the executives “trust existing systems over cloud-based systems due to the fear about security threats and loss of control of data and systems” (Circle ID Survey 2009).

These fears of cloud security are worsened by the legislative requirements that many countries impose on the responsible parties (entity that uses cloud services) as these have increased the risk from purely reputational to include fines and possible jail sentences.

The requirements of the Protection of Personal Information Bill (see table 3.1) regarding secure data processing and the impact of these requirements can only be addressed by investigating the how to enhance numerous security measures that can be employed to secure the cloud. The investigation will also extend to information security policies and good IT governance practices as they form an integral part of changing behaviour to secure information.

The investigation has to question whether cloud computing, taking into account the legislative requirements and the impact, can still be a viable option for businesses to process and store sensitive data. Each of the security processes studies will be compared to the requirement in the POPI legislation as it mitigates the legislative impact of the Bill. This comparison will form part of the conclusion to the study in Chapter 5.

The list of security measures is not complete or exhaustive as the security measures employed will vary based on the deployment model and service model of the cloud to be secured as well as the fact that the sensitivity of the data and the interfaces between the cloud parties (customer and cloud service provider) will not be standardised. For example a customer can use the cloud only for data storage and this will require different security measures by the customer and the cloud service provider than in the instance where software as a service is used as a service model and a web interface communicates directly into the cloud and computational request are performed by the cloud and returned to the user of the browser.

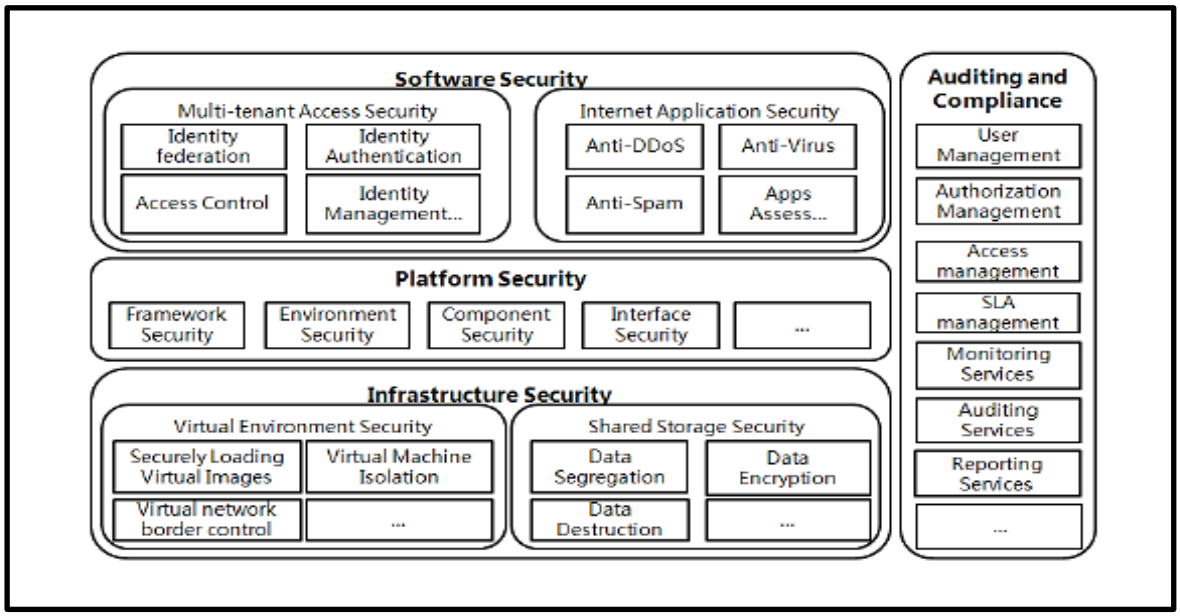
Subashini & Kavitha (2010) remarks that cloud computing moves application software and databases to large data centres where the management of this information might not be trustworthy. The challenges associated with

cloud computing are accessibility vulnerabilities, virtualisation vulnerabilities, web application vulnerabilities and physical access issues.

In order to address and investigate the vulnerabilities the cloud architecture has to be studied.

Figure 3.1 provides possible security solutions based on each level of the cloud architecture and based on the deployment model and service model some or all of these can be implemented to secure the cloud.

Figure 3.1 – Cloud Computing Security Architecture



Source: Chen & Zhoa, 2012

Each area will not be investigated separately as some areas will be combined in the study.

The first step into the investigation regarding the cloud is to identify the principles of what secure computing comprises by investigating both the requirements set out in the applicable ISO standards as well as promulgated Protection of Personal Information Bill.

The International Organisation for Standardization's Information Security Statement 7498-2 lists a number of suggested themes to be implemented that will result in secure computing (International Organisation for Standardization, 1989). The Proposed Protection of Personal Information Bill has similar themes (called "conditions" in the Bill) and prior to the discussion of the information security risks it is prudent to list and discuss the similarities regarding the two sets of requirements.

These similarities will be the overriding theme in any process, policy or technical security measure implementation as they form the basis and principles against which the effectiveness of the security measure will be measured.

Table 3.1 – Comparison of information security requirements in ISO 7498-2 and POPI Bill

ISO 7498-2 Requirements	POPI Bill 2009	Discussion
Identification and authentication	Accountability	Users of the cloud must be identified and access priorities and permissions may be granted accordingly.
Authority	Processing Limitation	Authorisation is an important security requirement in cloud computing to ensure referential integrity is maintained. Control has to be exerted over privileges and process flows to maintain the integrity of the data.
Confidentiality	Purpose Specification	Control of data over multiple distributed databases has to be maintained especially in a public cloud do to its accessibility over the Internet. Information security protocols have to be enforced over various layers of cloud applications.
Integrity	Further Processing Limitation	The integrity of data in the cloud is dependent on both the due diligence in accessing date as well as processing data.
Non-repudiation	Information Quality	Non-repudiation in Cloud computing can be obtained by applying the traditional e-commerce security protocols and token provisions to data transmissions within cloud applications such as digital signatures, timestamps and confirmation receipts services (digital receipting of messages confirming data sent/received).
Availability	Openness	This is one of the key components in deciding which cloud deployment model to use (public, private, hybrid or community) as the risk of non-availability has to be assessed. The risk can be largely mitigated by a service level agreement.
No requirement in ISO standard	Security safeguards	Chapter 4 of this study is dedicated to the security requirements of the Bill.

ISO 7498-2 Requirements	POPI Bill 2009	Discussion
No requirement in ISO standard	Data subject participation	This requirement is not addressed in the ISO standard, but in terms of the Bill a data subject must have the opportunity to amend his/her personal information.

Source: International Organisation for Standardization, 1989, South Africa, 2009

Both sets of requirements in the ISO statement and the Bill are similar and by addressing these requirements regarding secure information handling the quality and appropriateness of processes to be implemented can be measured.

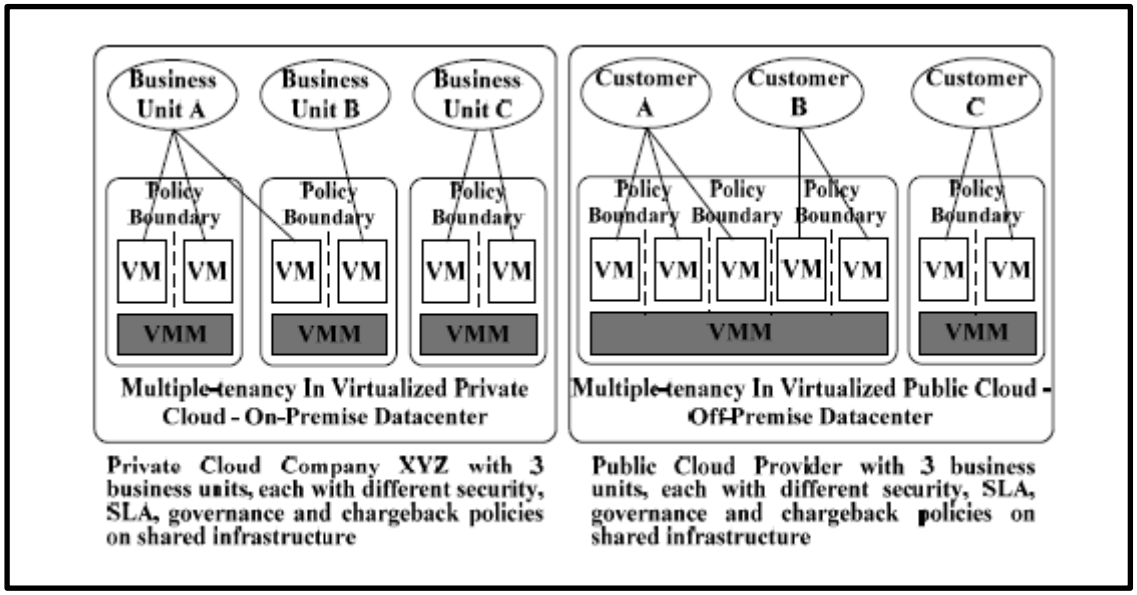
These principles identified in Table 3.1 can now be applied to a cloud environment by identifying the information security risks in the cloud environment and applying the principles to each risk identified the risk can be addressed and mitigated.

3.2) Identifying Cloud Computing Risks

Che *et al*. (2011) investigates the different security models that can be used to identify the risks and weaknesses in the cloud computing infrastructure. Based on the study four different models to identify the risks in a public cloud are identified and will be discussed:

a) Multi-Tenancy Model

Figure 3.2 – Multi-Tenancy Model in Cloud Computing



Source: Che *et al*. (2011)

Che *et al.*, 2011 discusses the Multi-Tenancy Model that allows multiple applications of cloud service provider to run on a physical server and offer services to customers. The physical server is partitioned and the user sees each virtual server as a single server. By partitioning a physical server into numerous virtual machines this "virtualisation" enables the sharing of computing resources such as processing, memory, storage, applications

and ensures that cloud resources are optimally utilized. The benefit of hosting different customer's applications and data on different virtual machines is that processing errors, viruses and malicious attacks can be isolated.

Multi-Tenancy has some complexities to it such as data isolation, architecture extension (flexibility and scalability), and configuration self-definition and performance customization. Data isolation requires that different customer's data do not come in contact with one another and that both processing and data storage is unique to each customer. The Multi-Tenancy model should provide a basic framework to implement a high degree of flexibility and scalability. The theme of configuration self-definition is based on the architecture extension principle as users/customers respective demands have to be supported. The Multi-Tenancy cloud has to enable the optimum utilization under different workloads and user requirements.

The Multi-Tenancy model security benefits are the fact that segmentation and isolation is obtained through the virtualization of a server. These benefits are also the risks associated with identified in this model.

The characteristics of segregation of data and multiple user access are the main risks that this model highlights, but based on where the servers performing the processing and data storage are situated regulatory compliance, storage and recovery of data could also be risk associated with this model.

The second model that Che *et al*. (2011) investigated where the Cloud Security Risk Accumulation model by the Cloud Security Alliance (CSA).

b) The Cloud Risk Accumulation Model of CSA

Che *et al*. 2011 remarks that the interdependent dependency on each layer in the cloud architecture has to be taken into account when analysing the risks in each layer. A weakness in a layer will influence the risk in that layer as well as the layer that is built using the weakened layer as foundation.

This risk identification model identifies the risk in each layer, starting at the physical layer the weaknesses and resulting risks in each layer is accumulated to result in a complete list of risks relative to each layer and the weakness in each layer.

The figure below depicts a wide list of technical security risks regarding the securing of data in the different layers/levels in the cloud, but the risks that are associated with cloud computing is wider than just data security as is discussed further in this section.

Table 3.2 – Cloud computing security risks

Layer	Service Level	Security Requirements	Threats
Application Layer	• Software as a Service (SaaS)	• Privacy in multitenant environment • Data protection from exposure • Access control • Communication protection • Software security • Service availability	• Interception of data • Modification of data at rest and in transit • Data deletion • Privacy breach • Impersonation (Man-in-the-middle attacks) • Session hacking • Traffic flow analysis
Virtual Layer	• Platform as a Service (PaaS)	• Access control • Application Security	• Programming errors • Software modification

	• Infrastructure as a Service (IaaS)	• Data security (data in transit or at rest) • Cloud management control security • Secure images • Virtual cloud protection • Communication security	• Software deletion • Impersonation • Session hacking • Traffic flow analysis • Connection flooding • DDOS attacks • Disrupting communications
Physical Layer	• Physical Datacentres	• No illegal abuse of cloud computing • Hardware security • Hardware reliability • Network protection • Network resources protection	• Natural Disasters • Network attacks • Hardware theft • Hardware interruption • Hardware modification • Misuse of infrastructure • Connection flooding • DDOS attacks

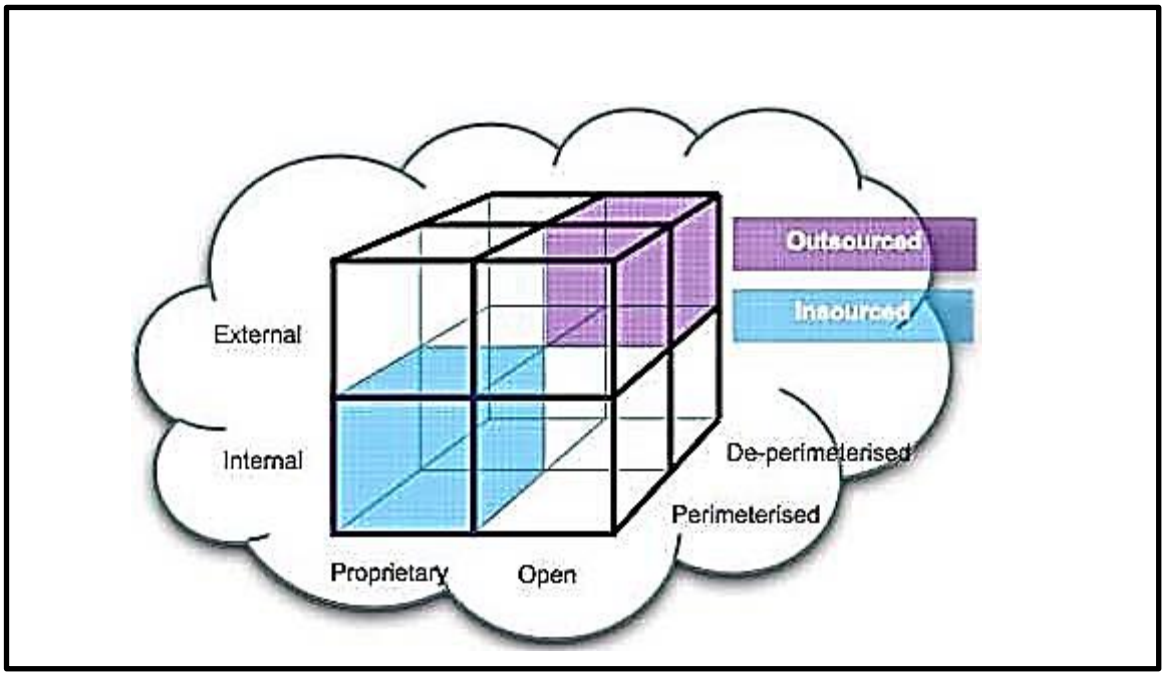
Source: Zissis & Lekkas, 2012 (Amended)

In table 3.2 it can be noted that numerous threats are similar across the different layers and that the security requirements are similar in some instances but also differ from layer to layer. Another method of identifying risk in the cloud environment is the Jerico Formu's Cube (Jerico Formu, 2009).

c) Jerico Formu's Cloud Cube Model

The third method of identifying risks in the cloud environment is based on the Jerico formu's Cloud Cube Model. This model uses a figurative description of the security attributes implied in the service and deployment models of cloud computing as well as indicating the location, manager and owner of the computing resources (Jerico Formu, 2009). The risk attributes of a specific cloud environment is influenced by these parameters and different combinations will result in different risk profiles.

Figure 3.3 – Depiction of the Jerico Cube



Source: Che *et al*. (2011), Cloud Computing Alliance, (2011) & Jerico Formu (2009)

Jerico Formu (2009), discusses the parameters of the cube and how each impact on the risk of the specific cloud configuration.

The parameters this method addresses are internal or external storage of data, the deployment model of the cloud meaning private cloud, public cloud or combination of the two (in this work it is called Proprietary or Open), and whether the security processes of the business applies to the cloud data.

- **Internal/External:** This parameter refers to the location the data is stored in the cloud. If the physical location of data is inside the data owner's boundary the model parameter is *internal*.

- **Proprietary/Open**: This parameter defines the ownership of the cloud's technology, service and interface. It indicates the level of portability of data between proprietary systems and other cloud components and the transforming of data between cloud components. The difference between *Proprietary* and *Open* is that in a proprietary cloud the provider holds the ownership of the cloud infrastructure and platform and customers cannot transfer their applications from one cloud service provider to another. In an *Open* cloud the technology are uniform which results in more competitive service providers and less constraints to integrate between different cloud and business partners.

- **Perimeterised/ De-Perimeterised:** This parameter defines the architectural design of the clouds security protection and whether a customer's application is inside or outside the traditional security boundary. Perimeterised indicates that the customers application is operating within the traditional security controls such as a firewall that limits movement of data between different security zones. De-Perimeterised refers to a less defined IT security boundary and requires the use of protocols to enable business to interact with each other without boundaries, irrespective of the location of the data or the number of collaborating parties. The Collaboration Orientated Architectures Framework (COA) sets out these protocols and requirements to implement a De-Perimeterised network.

- **Insourced/Outsourced:** This model parameter is in the 4th dimension and can be in two states in each of the eight cloud forms. *Insourced* refers to the cloud service being presented by the businesses own employees and *outsourced* refer to the service presented by a cloud service provider.

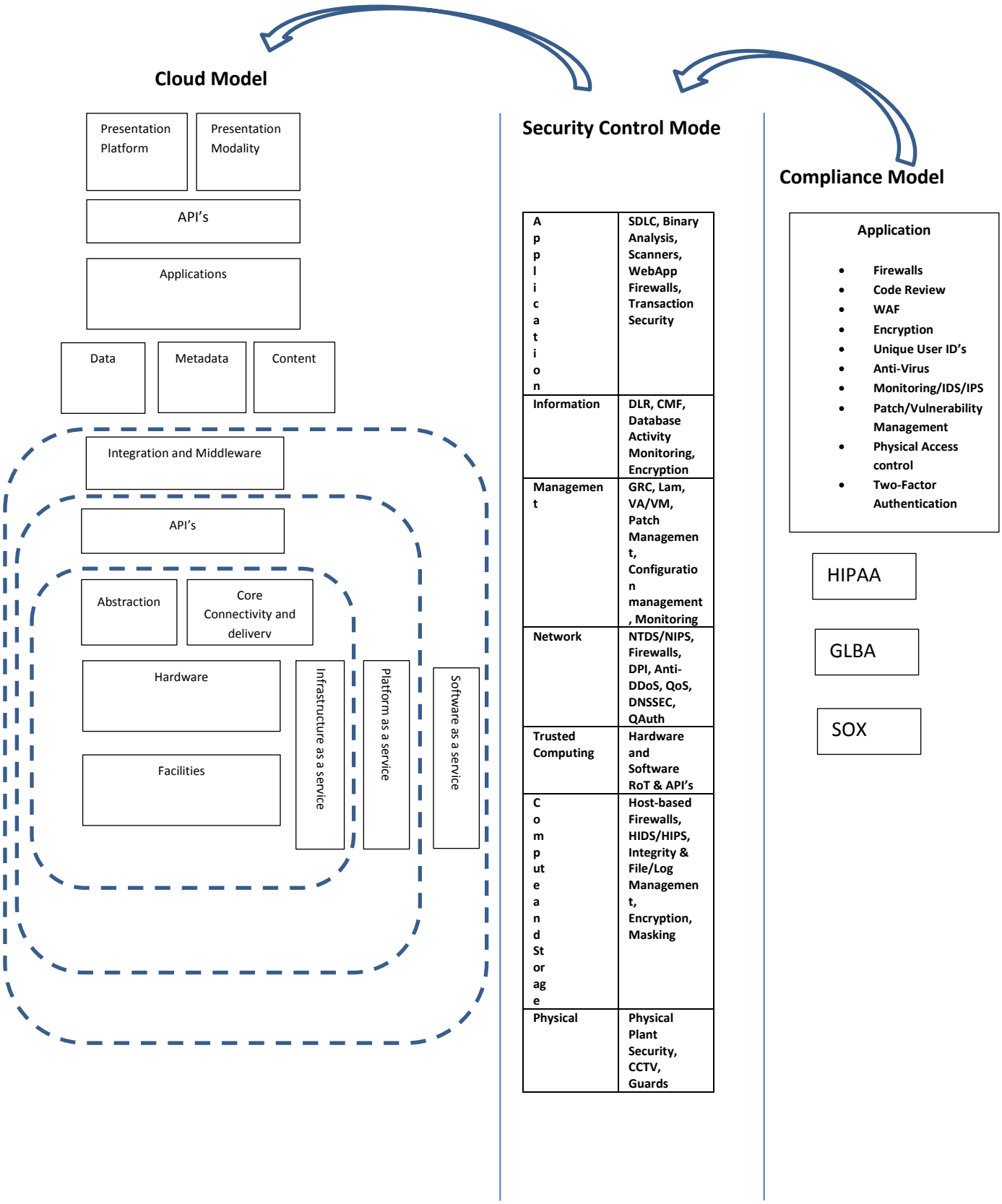
Additional attributes like Offshore and Onshore can also be added to increase the dimensions to identify risks (Che *et al*., 2011).

The final model is based on the principle of gap analysis where the gaps between the cloud infrastructure, the cloud security model and the overall compliance and information security management model is analysed and risks documented resulting from these gaps.

d) The Mapping Model of Cloud, Security and Compliance

The cloud mapping model is depicted in Figure 3.4 and identifies the gaps in security processes between the compliance, security and cloud model that results in data security risks.

Figure 3.4 – Depiction of the process of cloud risk mapping



Source: Cloud Security Alliance, 2011 & Che *et al*., 2011 (Amended)

Che *et al.*, 2011 discusses that the *mapping model* uses the different areas in the cloud (Architecture, security model of the cloud and the compliance requirements of the industry the cloud is active in) to identify and analyse gaps between the different areas and strategies. These gaps result in risks where one part of the cloud is not adequately secured in relation to either the compliance expectation or the current security model employed and unless addressed the cloud might be open for attack.

These models are primarily effective in identifying the data security risks, but the additional risks that cloud computing has, such as data recoverability and denial of service by the cloud service provider are discussed below.

3.2.1) Identified Cloud Computing Risks

Brodkin (2008) & (Foster, *et al.* 2009) identify a number of additional cloud computing risks based on the principles identified in the ISO statement and the Bill in Table 3.1. These additional risks are discussed below:

- **Regulatory compliance** > Customers making use of the Cloud service provider (CSP) is ultimately responsible for their own data in the cloud and where they are storing and processing personal information the onus is on the responsible party to secure this data. Service level agreements with cloud providers can assist in assigning responsibility and remedial action in case of breach. There is however privacy laws in various countries that requires sensitive data to be stored on a server that is physically in that country.

- **User Access** > As soon as data is communicated and processed outside the physical and logical controls of an organisation the inherent risk increases for unlawful access. The data communicated and stored in the cloud is dependent on the security measures and protocols that the cloud provider supplies. This can be managed and influenced by a strong service level agreement, but in case of a security breach the cloud provider might not be forthcoming with this fact as it will impact his business and tarnish the businesses reputation.

- **Data storage location** (Physical site of virtual server)> Users of cloud services might not know the physical location of the servers where their data is stored or where operation on the data is performed. When coupling this with the different data protection legislation in the different geographical areas it results in a high probability that the end user data might be physically in a country where the data protection legislation is weaker than the jurisdiction where the end users business is registered. An second complexity is that where a service provider does not return a user data at the end of the business relationship the legal enforceability of any SLA or other sections of the agreement between the User and the cloud service provider will depend on the interpretation of the laws and legal system in the countries that are involved (Country of origin of business and country where data is stored on server).

- **Segregation of Data** > The major benefits of cloud computing (cost and scalability) requires the cloud service provider to make use of virtualised machines/servers where numerous clients data is hosted on one server and the back end is shared with every user having the impression that their data is secure on a server. This results in clients' data being "next to each other" and if proper segregation and encryption is not present data could end up corrupted.

- **Recovery of data** > The data recovery risk is broken down into to focus areas. Firstly the need for the cloud service provider to have a robust Disaster Recovery Plan (DRP) is case of an emergency. This risk can be managed with a SLA, but if the plan is not tested or if it I not working and data is not available this can be detrimental to a business. Secondly the recovery of data when a business relationship ends has to be managed as the return or deletion of this data could impact the future confidentiality of the data.

- **Continuity of CSP** > Due to the nature of cloud computing the data that is being stored or processed are placed in control of the cloud service provider. If this CSP is not backed financially by a strong business that is economically viable the provider might disappear and any recovery of client data might be difficult to recover.

- **Investigative support** > Processing and data in the cloud could be stored over various servers and logging of processes for different customers will be difficult and any investigating any data leakage or any other form of data manipulation will be extremely difficult.

These risks are not exhaustive as the service model utilised by the user will impact some additional risks such as the CSP being able to view sensitive data to allow computations and processing in the cloud.

The principles of secure data processing has been studied and investigated in Table 3.1 and the general cloud computing risks has been identified as well as methods to identify these risks. The study now investigates the processes to address these risks by starting with the people aspect of data security namely the policies to manage information (Information Security Framework) and governance of the cloud environment moving on to the more technical areas of encryption, virtualisation and application security.

3.3) Information Security Framework

Data security has to be approached on an integrated basis across both the customer and the cloud service provider. To address the risk associated with the cloud environment a comprehensive approach to securing the cloud environment has to be followed consisting of a review and the implementing of an Information Security Framework, cloud governance processes and the technical security measures.

In this paper the security controls reviewed will be both from the view of the responsible party, being the controls that can be implemented during the data gathering process, as well as the controls that need to be present in the cloud service provider environment.

The human element poses the greatest information security threat to any organisation and has been disregarded in the past (Da Veiga & Eloff, 2007). The employees of an organisation are tasked to implement the policies and procedures designed by the organisation to control the associated risks. The risk that an employee might not comply with a key control is higher than the risk that a system, that is properly tested, would fail. The human element is complex as compliance breaches can be monitored but contrary to Information system monitoring this might happen after the breach has occurred as real-time monitoring of employees is difficult unless they interact with an IT system. This threat has to be addressed through policies implemented in the business and monitoring the output of the IT system.

The Information Security framework can be defined as a “comprehensive security model that ensures overall security of information there by eliminating business risks (Patil & Jagruti, 2008).

Guidance on what should be included and addressed in an information security framework can be found in the International Organisation for Standardization framework ISO/IEC 27001 (International Organisation for Standardization, 2005)

3.3.1) ISO/IEC 27001 - Information Security Management System

The objective of the standard itself is to "provide requirements for establishing, implementing, maintaining and continuously improving an Information Security Management System (ISMS)”. Its adoption should be a strategic decision. The design and implementation of an organization's information security management system is influenced by the organization's needs and objectives, security requirements, the organizational processes used and the size and structure of the organization.

ISO/IEC 27001 application results in the following objectives being attained:

- Formulation of the security requirements and objectives of an organization;
- Ensure cost effective management of security risk;
- Legislative compliance with laws and regulations;
- The statement can be used as a roadmap or process framework within an organization for the implementation and management of controls resulting in the security objectives of an organization being attained;
- identification and clarification of existing information security management processes;
- use by the internal and external auditors of organizations to determine the degree of compliance with the policies, directives and standards adopted by an organization;
- use by organizations to provide relevant information about information security policies, directives, standards and procedures to trading partners and other organizations with whom they interact for operational or commercial reasons;
- implementation of business enhancing and supporting information security principles;
- organizations can provide relevant information about information security to customers.

It is clear that developing an information security framework is to empower workforce and raise awareness regarding their responsibilities towards protecting the information assets of the business (Veiga & Eloff, 2007).

Corporate governance is those processes, technologies, customs and policies that direct how a business is administered and controlled. By utilising the cloud computing environment a business has to hand over some form of control over the information to a party outside the organisation and to do this confidently the internal governance processes as well as those of the CSP has to be reviewed.

3.4) Cloud Governance and Enterprise Risk Management

The fundamental issues of governance and enterprise risk management in cloud computing focusses on the identification and implementation of appropriate organisational structures, processes and controls to effectively implement information security governance, risk management and compliance with legislation (Cloud Security Alliance, 2011).

Information security governance has to form part of an organisation's overall corporate governance strategy and a well-designed information security governance process will result in security management programs that are scalable with the business as it grows, repeatable across different divisions of the business, sustainable, defensible and cost effective (Cloud Security Alliance, 2011).

Both the cloud computing customer (responsible party) and the cloud service provider has to develop information security governance, regardless of the service or deployment model utilised. The collaboration between the two parties should be based on agreed-upon goals.

The service model utilised may influence the defined roles and responsibilities in the collaborative information security governance and risk management (based on responsibilities defined) while the deployment model could influence the accountability.

Prior to entering into a cloud computing agreement with a service provider a due diligence process has to be done by the responsible party (customer) and specific security control needs to be identified and tested. The cloud provider's threat and breach detection capabilities has to be assessed and the continued implementation and maintenance of these processes has to be confirmed.

As part of the collaborative information security governance metrics and standards for measuring performance has to be established and the customer will need to investigate how its own security governance and processes will be influenced by moving into a cloud environment.

Risk management forms part of good governance and a thorough risk assessment has to be performed prior to moving a business into a cloud environment. As a minimum the risks identified earlier in this chapter has to be quantified and an appropriately measured by assigning an impact and a likelihood. This weighting assigned to each risk can to be increased or decreased as the controls and safeguards that the customer has insisted on in the SLA is taken into account as well as any other measures that will reduce the risk.

The use of recognised information security governance frameworks like COBIT 5 and the following cloud security standards will enhance the clouds governance.

- ISO/IEC 27017: Cloud Computing Security and Privacy Management System-Security Controls
- ISO/IEC 27036-x: Multipart standard for the information security of supplier relationship management that is planned to include a part relevant to the cloud supply chain
- ITU-T X.ccsec: Security guideline for cloud computing in telecommunication area
- ITU-T X. Srfcts: Security requirements and framework of cloud based telecommunication service environment (X.srfcts)
- ITU-T X.sfcse: Security functional requirements for Software as a Service (SaaS) application environment

The management and governance of data requires that data be classified in terms of its sensitivity and uses as this will govern the information management policies that will be applied to it. The classification will also assign ownership and custodianship to the type of information and authorised access or limitations will be governed and designed accordingly (Ranchal, Bhargava, Othmane, Lilien, Kim & Kang, 2012).

Both the Information security Framework and the cloud governance address the foundation of the securing of the cloud being policies and behaviour. The next part of the study addresses the technical security measures that can be used to secure the cloud.

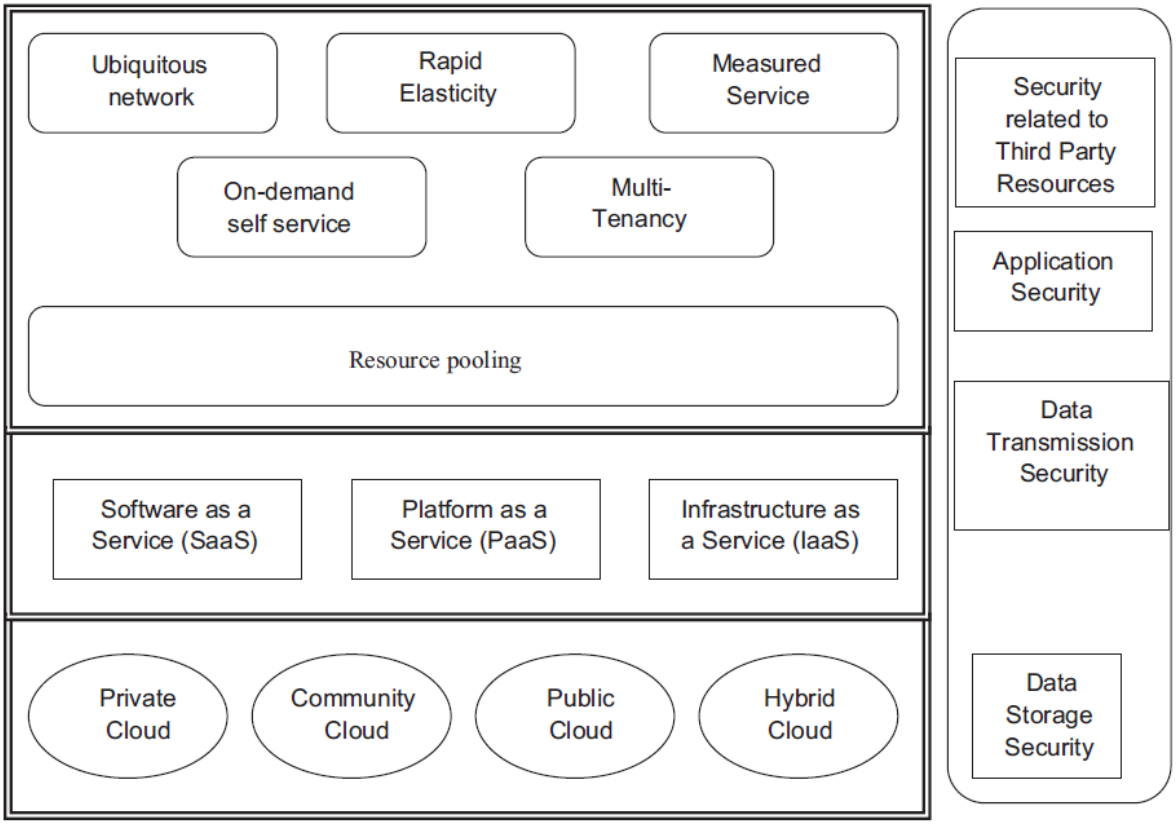
3.5) Operating in the Cloud (Security measures)

The security measures used differ based on the deployment and service model used in the cloud infrastructure under review. By first investigating the cloud architecture deployed the appropriate security themes and applications can be implemented.

3.5.1) Cloud Architecture

When reviewing the security in the cloud environment it is critical to analyse the structure of the cloud. Figure 3.5 depicts the cloud architecture and the data security that is applicable to the layer of the architecture. The Infrastructure as a Service layer (IaaS) is the foundation of the cloud with the Platform as a Service (PaaS) built upon the IaaS and the Software as a Service layer sits upon the PaaS. These layers are related as they form part of the same cloud structure and the weaknesses in the security of one layer influences the security of all the layers (Che *et al*., 2011).

Figure 3.5 – Cloud Architecture



Source: Subashini & Kavitha, 2010

The Cloud Computing Alliance (2011), explains the security interdependability of the different service models as follows:

IaaS provides the maximum extensibility for customers which results in limited security other than the infrastructures own security functions. At the IaaS layer it is imperative that the cloud customer take charge of security operating systems, software applications and data contents.

At the PaaS level customers can develop customised applications and build additional security into the applications and at the SaaS layer the security available is at the highest level and most integrated .

The principle is clear that the lower the service layer is the more management duties and security capabilities have to be performed by the cloud customer. If a customer is only making use of the SaaS layer of a cloud the cloud service provider would need to satisfy the requirements security, monitor and compliance but if a customer uses the IaaS or PaaS layer the responsibility to discharge the cloud security requirements will be with the customer as the cloud service provider is only supplying “availability” and elementary security such as access control to hardware.

The security responsibilities differ between cloud service models for example with Amazon’s Elastic Compute Cloud (EC2) (Amazon, 2010), included responsibility for securing the cloud to the hypervisor level. This results in the CSP only addressing physical security and virtualisation security. The user has to secure the OS, applications and data before it enters the part of the cloud infrastructure that the service provider takes responsibility for.

The study will not investigate the different levels of security and data protection assumed by different service providers and will discuss and investigate the security measures form an academic view point.

Different types of security will be discussed starting at the most detailed level being data encryption moving to secured virtualised environments and the security solutions that can be employed and on to application security and the different methods of identifying breaches in cloud security. The final part of the study will focus on Trusted Computing as based on Circle ID (2013) the perceived risk associated with cloud computing is too high for businesses to migrate to the cloud.

3.5.2) Encryption

In this section of the study focus will be on the technical aspects of securing data processing and communication in the cloud environment. The study is not exhaustive as a secure cloud can be achieved through various technologies and approaches but rather focussing on the general themes of encryption and continuing into data storage in the virtual environment and concluding with application security and intrusion detection solutions.

3.5.2.1) Types of Encryption

To secure the data in a cloud one of the main security measures is that of encryption both in the processing of data and in the storage of data. Encryption in its most basic form changes readable plaintext into an unreadable ciphertext. There are numerous different protocols to perform encryption. As part of the study we will be investigating the three basic encryption methods of hashing, symmetric cryptography and asymmetric cryptography.

- **Hashing Encryption**

Northcutt, (2008) states the fact that hash functions in cryptography is primarily to secure message integrity. The hash value provides a digital fingerprint that ensures that a message is not altered.

Hashing creates a unique fixed-length signature for a data set. Hashes are normally created with an algorithm and the hashes uniqueness to a set of data alerts the user to potential tampering.

The difference between hashing and other forms of encryption is that the process of hashing cannot be reversed or decrypted after it has been done. If a hash is compromised it cannot be used to decrypt the original message.

- **Symmetric Methods (Private-Key Cryptography)**

This is the most basic form of encryption (excluding hashing that cannot decrypt or encrypt data) based on the premise that to read a set of data a “private key” is needed to decode the cipertext (Dhir, 2000).

Private-Key encryption can be implemented in two ways namely a “stream” cipher and a “block” cipher dependant on the size of the data being encrypted or decrypted (Dhir, 2000).

A “stream” cipher encrypts or decrypts data one character at a time as it is transmitted while a “block” cipher encrypts and decrypts blocks of data as it is transmitted (Dhir, 2000).

Symmetric encryption algorithms like the Advanced Encryption Standard (AES) ((FIPS), 2001) and International Encryption Algorithm (IDEA) (Leong, Cheung, Tsoi & Leong,2000) or Triple-DES (Dhir, 2000) can be used.

The study into these different encryption algorithms is limited to understanding their working and application.

Symmetric cipher manipulates data sets (blocks or streams) by adding, moving, deducting or assigning different values to the ciphertext using a key or numerous keys in different rounds of manipulation. The obvious weakness in this process is if the private key is compromised during attack but for unsophisticated attacks with limited computing power large bit encryption 128 and higher will result in secured information.

The last part of the three encryption methods is asymmetric encryption.

- **Asymmetric Encryption**

Public key cryptography is more secure than symmetric methods of encryption. Cryptography of this nature uses two keys, a "private" key and a "public key," to perform encryption and decryption. The utilisation of two keys overcomes a major shortcoming of symmetric key cryptography, since a single key does not need to be securely managed among multiple users. (Wisegeek, 2013)

In asymmetric cryptography, a public key is freely available to everyone and used to encrypt messages before sending them. A different, private key remains with the receiver of ciphertext messages, who uses it to decrypt them.

A study of Fully Homomorphic encryption (Symmetric Encryption)will be performed as it is topical in the cloud environment where it will allow the CSP to perform data processing without being able to decrypt the data being processed an thus limiting any privacy compromises by the CSP.

- **Fully homomorphic encryption**

Ryan, 2012 states that with normal encryption data is encrypted before it is entered into the cloud. This limits the cloud provider’s ability to operate the data and results in the cloud being limited to a storage device. Homomorphic encryption allows the party that holds the ciphertexts to perform certain operations on the

cipertexts which mirrors the operations performed on the plain texts. In simple homomorphic encryption only one operation in the plaintext mirrors it in the ciphertexts.

There is however limitations regarding full homomorphic encryption in the cloud environment. The cloud computation result will have as an output the encrypted result of the data operations. This limits any further processing the cloud can perform based on the results as it cannot decrypt the result. A second limitation is that "big data" running this type of security encryption will result in large amounts of duplication as data will stored and processed locally as well as encrypted and processed in the cloud (Ryan, 2012).

Homomorphic encryption is a cipher solution where information stored and processing in the cloud needs to be isolated from the CSP due to its sensitivity. The two limitations mentioned above will need to be assessed and an additional constraint might be the network or Internet speed available in a country or area. If real-time computation is required this might not be a viable solution (Ryan, 2012).

Encryption secures the data that moves over networks by securing and confirming the right counter party has received the information. When the data however enters the cloud virtualisation and processing and data storage needs to be secure. The study now investigates the applicable security methods to secure the virtual environment.

3.5.3) Data Storage and Virtual Machines

One underlying mechanism enabling cloud computing is virtualisation, be it at the hardware, middleware, or application level (Christodorescu & Sailer, 2009).

Virtualization techniques are at the heart of Cloud Computing, and these techniques add their own vulnerabilities to those traditional in any connected computer system (Studnia, Alata, Deswarte, Kaâniche, Nicomette, 2012)

Gartner (2011) indicates that in 2012 around 60% of the virtualized servers will be less secure than the physical servers they replace, hopefully dropping by to 30% by 2015.

As the virtualization of infrastructure is such a large component of the cloud computing paradigm an investigation into different layers of virtualisation will be performed as well as touching on the building blocks of the virtual cloud and the security that can be implemented to secure the cloud.

Studnia *et al*., 2012 discusses different kinds of virtualization and based on the needs of the user. :

- **Process Virtualisation**: virtualizing this layer consists of providing an interface between an application and the underlying system. This allows for the programmer to create an application without being mindful of the specifications of the underlying operating systems it will run on as long as the application possess the correct virtualisation layer.
- **Server virtualisation**: Virtualization is applied to the hardware. In the cloud computing scenario this will allow numerous operating systems to run simultaneously on the same physical machine.
- **Network virtualisation**: VPN's (Virtual Private Networks) is the most common and enables private networks to interconnect through public infrastructure like the Internet and VLANS's (Virtual LAN's) where local networks share distinct physical infrastructure.
- **Storage Virtualisation**: SAN's (Storage area networks) consist of data storage devices where large quantities of data from different users are isolated and stored on the same device.

In order to understand and investigate the security solutions that can be implemented to secure the virtual machines that constitute a cloud some terms has to be explored and explained:

- **Full Virtualisation** – This type of virtualisation replicates a complete installation of one machine on another. The whole machine is thus replicated. The operating systems are unmodified and are only sharing hardware (Mishra, Mathur, Jain, Singh & Rathore, 2013).

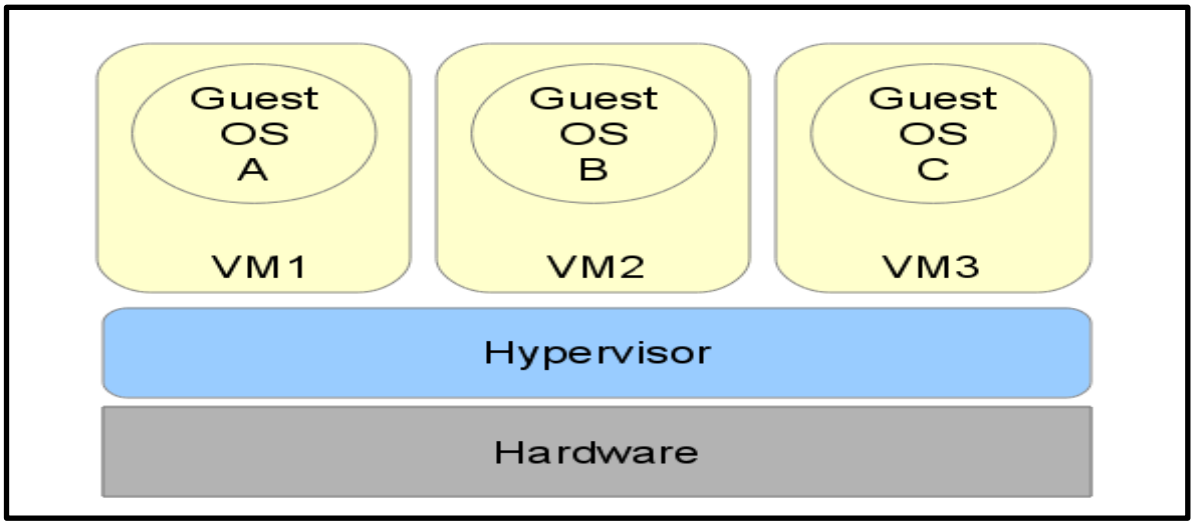
- **Paravirtualization** – This type of virtualisation allows multiple modified operating systems to run on a single server at the same time (Mishra *et al.*, 2013).

- **Emulation** – Similar to full virtualisation as unmodified operating systems are allowed to run, but with emulation the resources seen by the guest OS are completely simulated by software. The benefit of this configuration is that an operating system can be compiled on an architecture (virtualized) different from the architecture of a host.

- **Hypervisor Architecture** - A computer tool allowing various software applications running on different OSs to coexist on the same server at the same time. This means that Windows, Java, Linux, C++, Simple Object Access Protocol (SOAP) can operate concurrently on the same machine. The hypervisor is the enabling technology for server virtualization (Studnia *et al*., 2012) and (Mishra *et al.*, 2013).

Hypervisors can be installed on two levels, the first being above the hardware as can be seen below or alternatively above the an operating system that is running on the host hardware. By taking the figure below and placing another level of OS between the hardware and the hypervisor.

Figure 3.6 - Hypervisor placement in virtualised server environment



Source: Studnia *et al.*, 2012

The different methods to virtualise a cloud will each have its own security challenges, but the design goals of the virtual system can be standardised. With these principles and goals in mind a list of the minimum security features can be investigated in section 3.4.3.1.

The design goals of a virtualised system are discussed below. The list is not complete as there could be physical attacks at the server source that has not been addressed in this work (el-Khameesy & Rahman 2012 p.970 - 974).

- Accurate storage to ensure data is valid, accurate and complete which will result in data dependability.
- Identification of data errors should be effective and the locating of a malfunctioning server should be a relatively easy process.
- Continued data support resulting in data being as secure after being used (modified, deleted or appended) by users.
- Monitoring to allow users to perform storage accuracy checks.

By comparing these design goals to a virtual environment the implementation of security controls to address the weaknesses in the current system will become apparent.

3.5.3.1) Virtualization Security

The methods to secure the virtual environment are numerous and there are various technical solutions that can be implemented. The list below is of a general nature and solutions are available representing each of these security themes.

Virtualization security should consist of the following (El-Khameesy & Rahman 2012 pp.970 - 974):

- Authentication schemes provided by the OS should be evaluated. Systems that encrypt and authenticate communications should be preferred.
- Secure access through authorisation list and strong password requirements. A two-factor authentication can be used combining usernames and passwords with secure tokens and biometrics.
- Updating security and malware software based on published new threats such as the SANS Security Alert Consensus.
- Logging and auditing controls should be implemented to serve as a deterrent to internal and external breaches.
- Network security such as Firewalls and an IDS device that filters traffic has to be implemented.
- Isolate the management of the virtualisation from the storage virtualisation.
- Monitor unusual data flows and activities.
- Implement port binding switches to prevent World Wide Name spoofing. The control is to bind the specific switch port allowing only connections of that device through the pre-defined port.
- Disable access through insecure protocols like HTTP and force only secure encrypted communication through HTTPS.

All of the above controls have to be monitored for effective implementation and continuity.
By implementing the above principles a secure virtual environment could be secured but without effective monitoring new malware might render the current solutions obsolete in a short period of time.

By effectively identifying breaches through VM monitoring the virtualised data base manager can protect the VM environment.

3.5.3.2) VM Monitoring

VM Monitoring is one solution to protect against the different possible attacks that can be performed in the virtualised environment.

Below are some forms of VM monitoring and how it protects the virtual machines.

3.5.3.1) Virtual Machine Introspection (VMI)

VMI refers to techniques that allow the hypervisor to access virtual memory in order to analyse its content from the outside. The retrieval and analysis of data can be done directly in the hypervisor or from an outside dedicated virtual machine. There are limitations to this solution as the virtual machine monitor (VMM) does not have any knowledge of the principles used by the guest OS and cannot interpret the retrieved data. (Studnia *et al.*, 2012)

The limitation described above is the reason for the existence of a VMI and the additional controls they implement to monitor the guest OS. Some of the additional controls are:

- **Monitoring or interfering** – can the VMI only monitor anomalies and report them or can it protect the VM by reacting to an attack.
- **Event reply** – this allows the VMI to record the state the monitored virtual machine is in for further analysis similar to cloning to VM.

The second process in using VM monitoring is Kernel Protection.

3.5.3.2) Kernel Protection

By virtualising the OS it is placed is a less privileged state as the hypervisor is assigned the highest privileges. This allows the hypervisor to enforce security on the OS. By implementing a VMM the hypervisor is limited to only executing approved code (Studnia *et al.*, 2012).

An example of this type of VMM is SecVisor (Studnia *et al.*, 2012) which does not stop code from being added to the kernel, but it will not execute the code unless it is approved first.

Another form of VM monitoring is “rootkit detection” and is explained below.

3.5.3.3) Rootkit Detection

The rootkit detection method is designed to detect rootkits hiding in the monitored OS without impacting the OS capabilities (Schultz, 2008).

The process of rootkit detection requires the code of the virtualised OS to be market as non-executable, which then triggers an action from the hypervisor the first time the code is executed since it has been modified from its previous execution. The code is now compared with a database of known binaries. This results in the detection where code or binaries has been modified in the OS (Studnia *et al.*, 2012).

Another method of securing the data in the cloud is by saving data in different parts of the virtualised network. This is known as Data Dispersion and will hamper any attacks, but will also slow done the recovery of the data as time will be lost due to the parts of the date needing to be recovered.

The storage of data in the virtual network has been investigated and if the responsible party uses SaaS the information source into the cloud will be a web browser. The study now investigates the application data security level of the cloud infrastructure and the possible mechanisms to use to secure this area.

3.5.4) Application security

The two most common technologies to access the IaaS, Paas and SaaS services are through Web Services and Web Browsers (Jensen, Schwenk, Gruschka & Iacono, 2009).

Web Service is used to provide access to IaaS infrastructure and Web Browsers are used for SaaS. In the PaaS environment both technologies can be found.

3.5.4.1) Web Service and Browser Security

The use of HTTPS together with WS Security should be the minimum when accessing the cloud (Ramgovind, Eloff, & Smith, 2010).

Jensen *et al.*, (2009) investigates how to provide integrity, confidentiality and authentication in web services.

Web browsers rely on different protocols to secure communication to the cloud. If these security measures are compromised the browser can allow unauthorised access into the cloud network.

The securing of a browser is dependent on the integrity of the browser's own code which can be managed with Origin Policy Controls and the second being to protect sensitive user data being accessed or modified by malware.

- **Origin Policies Controls**

Origin Policies limits and controls changes to the script to the original application (same domain, name, protocol and port) that created the script has to make changes to the script. (Karlof, Tygar, Wagner & Shankar, 2007).

Separation of managed identities of the cloud consumer from those of the cloud provider must be ensured to protect the customer's resources (information) from provider-authenticated entities that access that data (Jansen & Grance, 2011).

- **Web Authentication Protocols**

Standard protocols for communication between the browsers over the internet to the cloud have been studied and a short discussion on the most common protocols follows below.

Web browsers use SOAP messages to communicate to the cloud, but by using XML Signature and XML Encryption these messages can be secured (Jensen *et al.*, 2009) & (Jansen & Grance, 2011)

The XML signature assigns an element to every message and this part is hashed and canonicalized (converting data into a standard format). This hashed element is added to the security header of the message.

XML Encryption defines an encrypted key for transportation purposes. The most common encrypted key used is a hybrid encryption where an XML fragment is encrypted with a randomly symmetric key which then in itself is encrypted using a public key. In a SOAP message the encrypted key will appear in the header (Jensen *et al*., 2009).

The terms SOAP and XML language is briefly discussed as it is such an important part of the controls over browser application security.

- **SOAP (Simple Object Access Protocol)** – XML messaging framework designed to allow heterogeneous applications to exchange structured information in a distributed environment. SOAP

usually relies on HTML (Hypertext Transfer Protocol) or SMTP (Simple Mail Transfer Protocol) (Jansen & Grance , 2011).

- **XML (Extensible Markup Language)** – Is a markup document language that defines the rules for encoding documents in a format that is both readable by humans and machines. The "markup" refers to a system of annotating a document which is distinguishable from the text through syntax's. This results in the software carrying out operations on the text that is not displayed to the users. HTML (Hypertext Markup Language) results in pre-defined presentation semantics which results in specifications how structured data is to be presented (Jansen & Grance (2011).

The next secure protocol that was studied is the Transport Layer Protocol which is extremely popular as HTTPS is based on this security verification system.

- **Transport Layer Security (TLS)/Secure Sockets Layer (SSL)**

TLS and its more common name Secure Sockets Layer are cryptographic protocols designed to secure communication over the Internet. *HTTP over SSL is also known as HTTPS* (Karlof *et al*., 2007) The security is based on **X.509** certificates which assures counter party authentication and uses symmetric keys to exchange information (Jensen *et al*., 2009) and (Karlof *et al.*, 2007).

The Record Layer Encrypts or decrypts TCP (Transmission Control Protocol) data streams using keys agreed upon during the *TLS Handshake* (Authenticate server and client).

The following is an example of how TLS will ensure Web browser security using encryption and authentication of network peers:

Web server is configured using X.509 certificates that includes domain name. The certificate has to be issued by a "trusted" certification authority (CA).

During the TLS *Handshake* the server sends the certificate to the browser. The browser verifies that the certificate has been issued by a "trusted" CA and that the domain name contained in the certificate matches the requested URL.

As part of the study a short investigation into the components of TLS was done in order to better understand its workings.

- **X.509** – The ITU-T (International Telecommunications Union – Telecommunications Standardization Sector) standard for public key infrastructure. X.509 specifies standard formats for public key certificates, certificate revocation lists, attribute certificates and certification path validation algorithms.
- **Transmission Control Protocols (TCP)** – Provides reliable, ordered, error-checked delivery of data between programs running on different computers connected to a LAN, intranet or the Internet. TCP thus guarantees that all bytes received by one computer will be equal to all bytes sent in the correct order. The method used to guarantee the secure transfer works on the bases that the receiver of the packet data will acknowledge receipt and a the sender keeps record of each packet sent as well as tracking the time elapsed since sending and receiving a positive confirmation back from the receiver. If a packet's timer expires TCP will resend the packet of data.

The last method of securing the browser is the key translator in the browser.

- **Key translation in the browser**

This method of securing the browser requires that data is encrypted before being uploaded into the cloud and the data owner retains the key (Ryan, 2013).

To protect a client from malicious software the connection to the cloud has to be authenticated. This cannot be done by XML tokens as browsers cannot generate cryptographic tokens. A trusted third party help is needed to generate the security required. When the browser cannot authenticate a user a HTTP redirect is sent to the third party who authenticates the details of the "log-in" and supplies the browser with another HTTP message to allow access.

The downside to this type of encryption is that it limits the processing that the CSP can perform as he never has any access to the decrypted data and the results in the cloud being limited to a storage and forwarding tool.

Intrusion detection in the cloud environment is important to the responsible party or user as control over the data is given to the CSP and unless the responsible party or user is informed of any breaches to corrective action can be taken. Attacks can originate inside or outside the organisation. To allow the user some form of comfort that data is secured the CSP has to implement reporting software or hardware to inform the CSP that an attack happened or is currently happening.

3.5.5) Cloud Intrusion Detection

The goal of intrusion detection is to identify, preferably in real time, unauthorised use, misuse, and abuse of computer systems by both systems insiders and external penetrators (Mukherjee, Heberlein & Levitt, 1994).

Intrusion detection is defined to be the problem of identifying individuals who are using a computer system without authorisation and those who have legitimate access to the system but are abusing their privileges (insider threats).

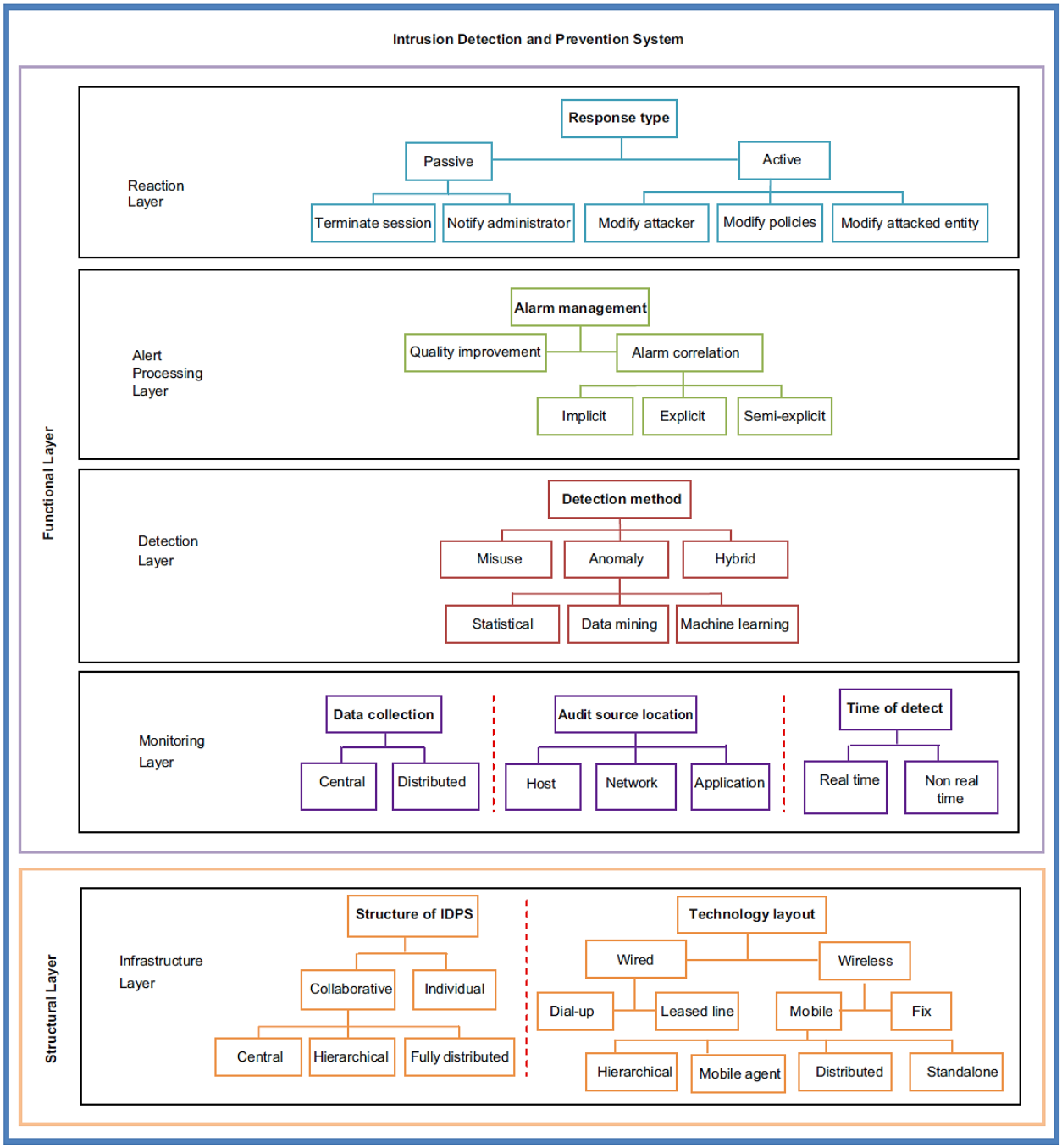
Possible attacks at the network layer of cloud computing are IP Spoofing, DNS Poisoning, man-in-the-middle attack (MITM) or port scanning (Modi, Patel, Patel & Rajarajan, 2012). A short study into these types of attacks is necessary to form an understanding how the cloud can be compromised.

- **IP Spoofing** – The attacker creates Internet Protocol (IP) packets from a fraudulent source IP address. The header of each IP packet contains the source and destination address and by manipulating the source the attacker can create the appearance that the IP was sent from a different computer (Modi *et al*., 2012).
- **DNS (Domain Name System) Poisoning ("Pharming" attacks)** – An attacker insert a fake address record for an Internet domain into the DNS. The server accepts the fake record and subsequent requests for the address of the domain are answered with the server controlled by the attacker (Modi *et al*., 2012).
- **Man-in-the-Middle attacks** - The attacker creates the illusion to independent connections that they are talking to one another where they are actually communicating to the MITM. Information is requested form the connections and fraudulently used (Modi *et al*., 2012).
- **Port Scanning** – This type of attack dispatches client requests to a range of server port addresses on a host, with the goal of finding an active port exploiting a known vulnerability of that service (Modi *et al*., 2012).

A study of the different types of intrusion detection software and ideas are set out below.

Intrusion detection can be performed at the network, host or application layer. In the figure below the possible working of an intrusion detection and prevention system can be seen.

Figure 3.7 – A layered-taxonomy of IDPS



Source: Patel, Taghavi, Bakhtiyari, & Júnior, 2013

Based on figure 3.7 there are two types of intrusion detection software. **Intrusion Detection Software (IDS)** automates the intrusion detection process where as **Intrusion Detection and Prevention Systems (IDPS)** is either a software or hardware device that has all the capabilities of an IDS system but can also attempt to stop possible incidents (Scarfone & Mell, 2007).

The working of intrusion detection software or hardware is based on the premise that an intruder's actions and behaviour will be notably different from a legitimate user.

IDS requires that the model or also called signatures of intrusion is defined resulting in the IDS knowing what to look for. There are two types of models. The first is called an "anomaly" detection model and the second is the "misuse" detection model (Patel *et al.*, 2013).

3.5.6.1) Anomaly Detection Model

This model bases its detection parameters on the user or group of user's normal behaviour. The IDS will statistically analyse the user's current session, comparing it to the profile representing the user's normal behaviour and will flag significant deviations or anomalies (Patel *et al.*, 2013).

3.5.6.2) Integrating Signature Intrusion detection Software (Misuse detection model)

This model compares the user's session and/or command against a pre-defined set of signatures/ or attributes that attackers use to penetrate a system. If a pattern is identified that is known to cause security problems the session is flagged. This form of detection is not as effective due to the time lag between new threats being introduced by penetrators and the list of signatures and attributes being updated in the IDS software (Patel *et al.*, 2013).

3.5.6.3) Monitoring data access

There are two broad types of software that can assist the CSP in this regard. The use of Database Activity Monitoring (DAM) software and File Activity Software (FAM) will highlight the fact that data has been moved into the cloud from the local network.

Database Activity Monitoring software refers to a suite of tools that can be used to support the ability to identify and report fraudulent, illegal or undesirable behaviour, with minimum impact on user operations and productivity (Gartner IT Glossary, 2013).

File Activity Software can identify excessive user access, audit file access based on user rights as well as alert the business if user requests violate corporate policies.

An additional protection is the use of URL (Uniform Resource Locator) filters where the interface with the cloud is only available to authorised personal in a business. The administrative interfaces for the cloud would use a different URL than the consumption/user would use and the URL filter can distinguish between the different URL's to allow user access.

3.5.6.4) Data Loss Prevention Software (DLP)

The difference between IDS and DLP is that DLP software identifies sensitive and critical data and either blocks this data from being communicated over a network or alternatively allow the communication but flag it as a breach to the administrator (SANS Institute Data Loss Prevention, 2008).

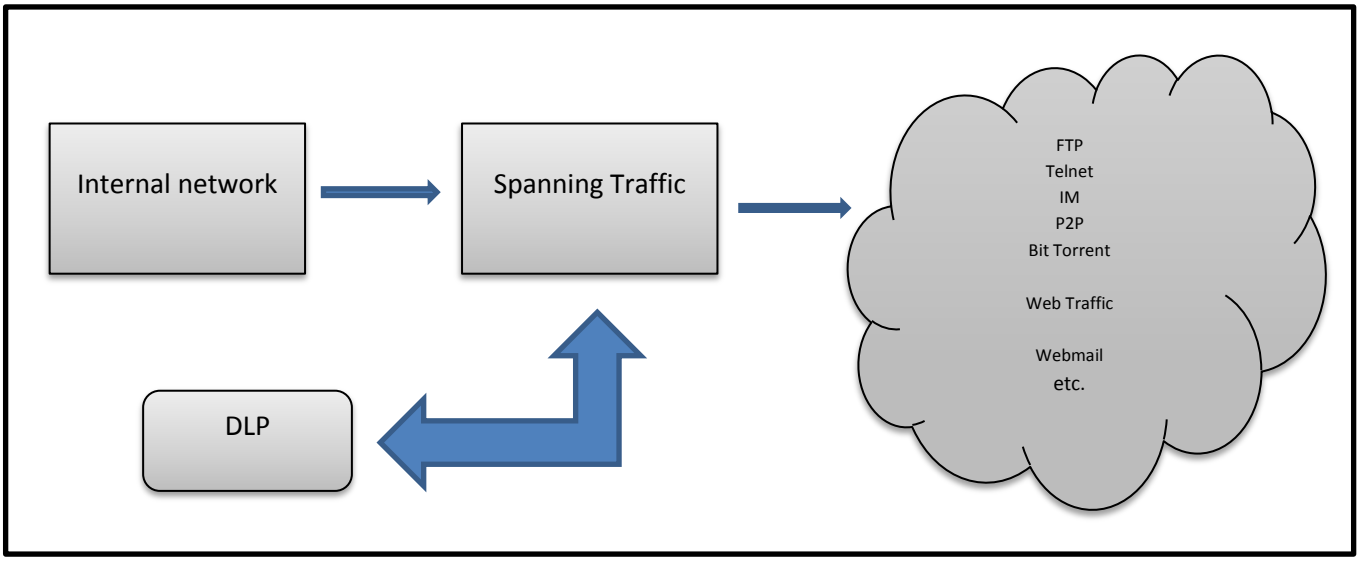
A DLP system requires that information to be monitored be designated as sensitive as all communication will not be monitored. Each business will have unique parameters as to what type of information it identifies as sensitive, but for the purposes of this work the definition of "personal data" as defined in The Protection of Personal Information Bill could be used as a guideline.

The DLP solution can monitor activity in different areas or actions in a network, either when data is moving over the network, data that is stored (saved) or during e-mail conversations.

These three areas where sensitive data are monitored are now discussed and graphically depicted in figures 3.8 and 3.9.

- **Data on the move** – Monitoring of all data traffic moving over lines leaving the internal network of the business. The monitoring takes place as soon as data is communicated outside of the businesses internal network. The sensitivity level of the data will either trigger the DLP process or allow the data to be communicated and flag it or block the communication.

Figure 3.8 - How a DLP monitors while data is moving over a network



Source: SANS Institute Data Loss Prevention, 2008 (Amended)

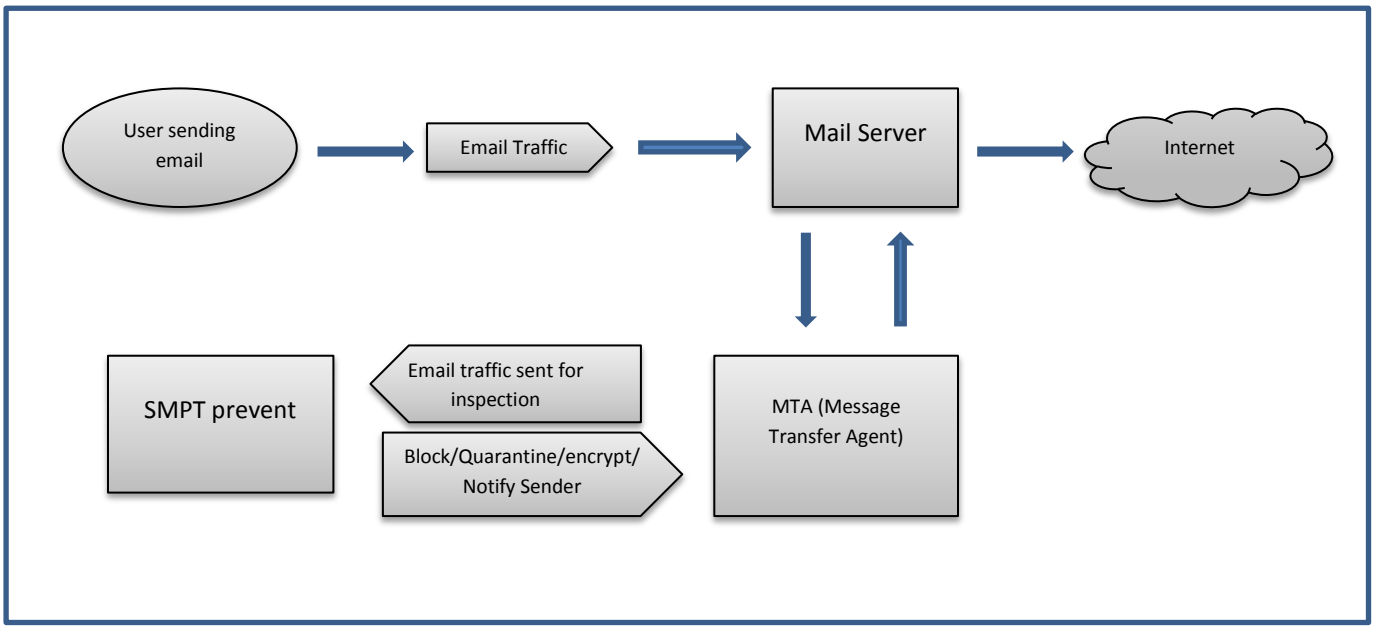
A further control that the DLP process allows a business is that of limiting data to leave the network via USB or other storage devices. The DLP could monitor all data leaving the network via communication over a network or to a physical device. This monitoring of physical devices is called Data End Points monitoring and it is briefly discussed below.

- **Data at end points** – This application is installed on end user workstations and laptops monitoring any data leaving via removable devices such as USB drives. Additional to monitoring devices it provides auditing logging and protection against users printing sensitive data.

- **Data stored** – Applies to monitoring databases and files to identify sensitive data stored in areas of the network where the security is insufficient or copies of sensitive data stored by an unauthorised person. The DLP will scan databases for designated sensitive data and when a copy of these sensitive files are found in a area that has not been designated the database administrator will be informed. Some DLP software solutions will even move a sensitive file to a different secure location if the monitoring activity has flagged that the file is at risk.

- **E-Mail Transmissions -** In Figure 3.9 the working of DLP monitor regarding e-mails are depicted. In regards to electronic mails the standard transmission protocol of SMPT (Simple Mail Transfer Protocol – most common standard for email transmissions across the internet – text based where recipients of communication are specified and verified that they exist.) and integrating into message transfer agent (MTA-software that transfers electronic messages from one computer to another) any message is intercepted by the DLP at the outgoing mail server and then re-rooted for inspection prior to being sent to the MTA for communication outside the network.

Figure 3.9 - How a DLP monitors e-mail transmissions



Source: SANS Institute Data Loss Prevention, 2008

Mackay, Baker & Al-Yasiri, (2012) investigated the reasons why there has not been a massive move to cloud computing infrastructure and found that the customers does not trust the cloud service providers sufficiently to move their information into the cloud. A solution to obtain the trust required to move data or processing into the cloud is to implement a "Trusted Computing Platform" into the network.

3.5.6) Trusted Computing platforms

Mackay *et al*., (2009) introduces the concept of Trusted Platform Computing. Trusted Computing (TC) is a specialised field of trusted systems whereby a device is made to behave in a consistent, predictable manner enforced by hardware and software techniques such as cryptography and automated authentication (Trusted Computing Group, 2011). TC ensures that only authorised code runs on a system and this ensures critical data is protected.

In the cloud environment trusted computing will be implemented through encrypted data storage, memory curtaining (Hardware enforced memory isolation where different programs cannot read data from one programs memory to another) and specialised TPM (Trusted Platform Module) architecture to securely virtualise environments (Ryan, 2013).

In the cloud environment TC allows a cloud to authenticate it to other known machines. The security measures that TC uses can unfortunately also prevent and restrict access for users and systems that are valid, but does not follow the requirements of the TC environment.

TC requires six key technology concepts to fully encompass a fully trusted system. They are as follows: Endorsement keys, secure input and output, Memory curtaining/protected execution, sealed storage, remote attestation and trusted third party support (Trusted Computing Group, 2011).

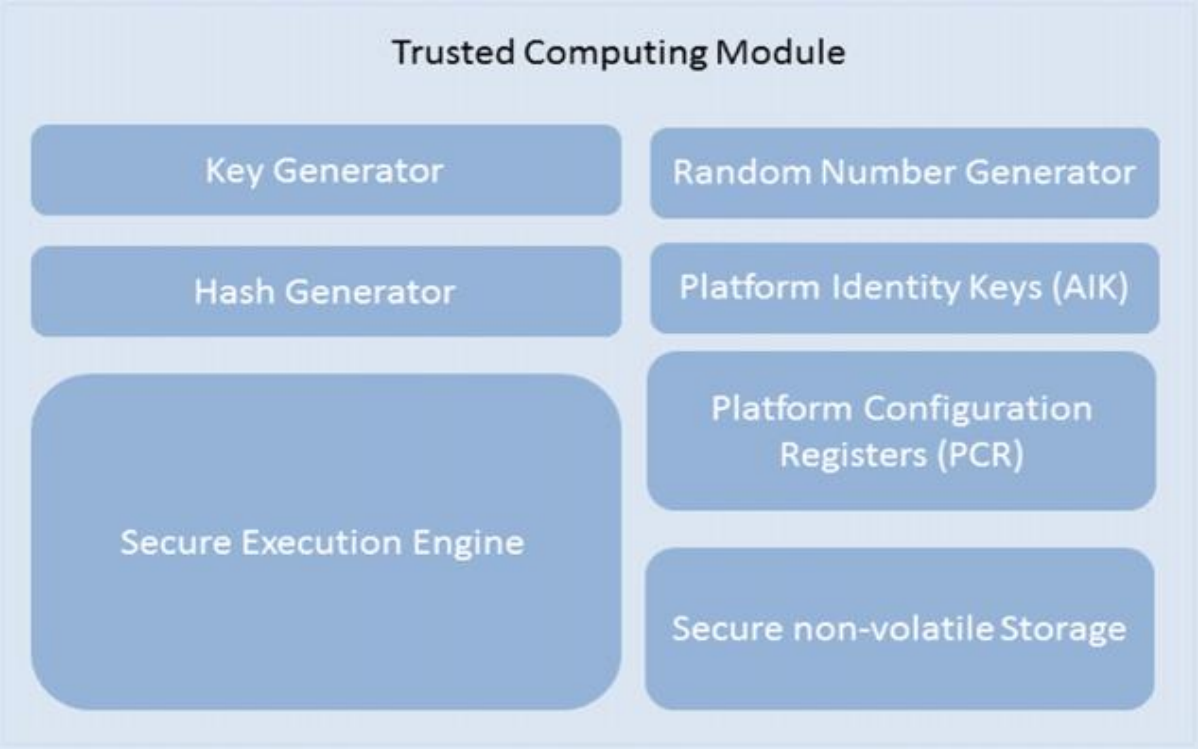
A TPM module is a special purpose microcontroller or chip that is designed to interface with standard hardware/software and is usually surface mounted on the motherboard of a PC. The TPM chip access the main bus of the computer which then allows it to track and report on the configuration state of the entire computer. By being able to report the state the computer was in when encryption was being performed the chip guarantees that security during the specified process. For example if a computer is used in a certain “trustworthy” state the TPM can then grant access to encryption keys as well as communicating to other computers in the cloud or network that it is currently being operated in this trustworthy state. As part of the TPM functionality it will include command infrastructure and protocols to migrate data between trusted devices (Trusted Computing Group, 2011) and (Ryan, 2013).

The trusted computing platform supplies a viable option regarding securing the cloud and the sensitive information that might be processed or stored. It consists of parts of security architecture like hashing and secure data storage that has been investigated earlier in the chapter and the only differentiating characteristic is that a TPM can be used to secure the execution of commands (Trusted Computing Group, 2011).

This effectiveness of this solution will depend on the cloud model as a Software-as-a-Service (SaaS) user will probably not be interested in this type of security.

Figure 3.10 represents a typical trusted platform. The security controls are similar to the list of controls proposed to secure the cloud environment in Chapter 3 with the addition of the “Secure Execution Engine” that is in the form of a TPM.

Figure 3.10 – Trusted Computing Module



Source: Trusted Computing Group, 2011

Based on the investigation conducted in Chapter 3 there are numerous methods to secure the cloud. The study has identified the requirements for data security in Table 3.1 and based on these the investigation was performed.

The investigation resulted in the following findings:

- Securing the cloud computing environment requires more than just a technical approach and ideally and integrated data security plan will have to be implemented. This would include IT governance processes, IT risk identification as well as an Information Security Framework.
- The human element and interaction regarding data security is as important as the technical data security controls implemented by a business. Humans are tasked to implement the controls and if there is no supporting policies and procedures such as an Information Security Framework they pose a similar risk to sensitive data being accessed without authorisation from outside the business.
- The security safeguards requirement of the POPI Bill can be discharged by implementing encryption, virtual machine monitoring, application security, cloud intrusion detection and possibly moving to trusted computing. The level and complexity of the technical controls that a business has to implement will depend on the deployment model and service model used, the cloud service provider own controls and the sensitivity level of the data that is processed or stored in the cloud.
- Due to the penalties imposed by the POPI Bill business will have to increase the security controls regarding sensitive data. This will result in additional cost as more sophisticated measures might be required to secure data in the cloud.

- The mistrust of businesses of cloud service providers regarding the recoverability of data, corruption or up-time will result in additional cost as organisations try to protect themselves through a SLA.
- The physical placement of the cloud servers could result in the CSP and the client having different business objectives. The CSP will place the physical infrastructure in the country where communication costs are the lowest to increase profitability, but the client will require that the servers are located in a country with the same or increased level of privacy legislation.

The data security controls that can be implemented to secure data are dependent on the cloud infrastructure as the risks and solutions associated with every cloud will differ. Securing data in the IT environment is not new and numerous solutions are available but cloud computing does add some complexity in regards to sensitive personal information as the risk is as high from outside attack as it is from the CSP using the without authorisation.

The additional risk of compliance with the promulgated POPI Bill will now be investigated and based on the findings in Chapter 3 an understanding of what will be required to comply with the requirements will be attained.

Chapter 4 – Implications on the Cloud Computing environment of the proposed Protection of Personal Information Bill

4.1) An Introduction to The Protection of Personal Information Bill

The South African National Assembly passed the Protection of Personal Information Bill (POPI) on 20 August 2013 after more than 4 years of deliberation (Cornish, 2013).

The Protection of Personal Information Bill aims to give effect to the constitutional right to privacy by ensuring that organisations process personal information in a fair, responsible and secure manner. The impact of this Bill on responsible parties and cloud service providers has to be investigated as an increased number of businesses embark on using cloud computing to process sensitive information. The Bill assigns responsibilities and specific requirements, to both the responsible party and the cloud service provider, and the study will highlight these major requirements and refer the reader to the relevant data security controls that can be implemented to discharge some of these requirements.

Organisations that fail to safeguard the personal information of customers, employees and other stakeholders could find themselves facing civil liability claims, criminal and regulatory sanctions and significant reputational damage.

The purpose of the Bill is two-fold, enhancing local privacy regulation as well as prescribing data protection practices in South Africa that are on par with international practices (PWC, 2011).

The responsibilities in term of the Bill to comply with the "Conditions for lawful processing of personal information" rests with two parties namely the "responsible party" and the "operator" (see definitions below as per the Bill).

As the cloud computing paradigm shift is taking place and more and more entities are contemplating a move into virtualization and cloud services the legislation governing especially the services provided by the "Operators" (Cloud Providers) are increasingly more topical as the benefits of scalability and cost reduction can be reduced if the compliance burden is too high.

In order to understand the implications of the proposed Bill a clear understanding of the services, their deployment (structurally and geographically) as well as the information security protections employed by a service provider has to be obtained. In the case where a principle service provider relies on sub-contractors the same assurances and warranties will have to be in place as with the principle service provider.

The different international legislation has assisted South Africa in compiling the POPI Bill and below we will study the different contributing Act's and principles the legislators has used to base the South African legislation on.

4.1.1) Processing Personal Information in Foreign Jurisdictions

Historically the Organisation for Economic Cooperation and Development (OECD) compiled "Recommendations of the Council Concerning Guidelines Governing the Protection of Privacy and Trans-Border Flows of Personal Data" (PWC, 2011). The European Union has adopted these recommendations, whereas the USA has opted to

promulgate sector specific bills regarding personal data protection as can be seen below (Heyink, 2012) and (Sotto, Treacy & McLellan, 2010):

- The Gramm-Leach-Bliley Act (Also known as the Financial Services Modernisation Act) requires financial institutions to protect the non-public personal information of financial consumers from disclosure.
- The Health Insurance Portability and Accountability Act ("HIPAA") and the Health Information Technology for economic and clinical Health Act ("HITECH") govern the protection of personal health-related information.
- Sarbannes Oxley ("SOX") governs internal controls over financial disclosures and the Federal Information Security Management Act ("FISMA") governs how federal agencies are required to protect personal information.
- The Fair Credit Reporting Act ("FCRA") and Fair Accurate Credit Transactions Act ("FACTA") requires consumer credit reporting agencies to implement reasonable procedures that are fair and equitable to the consumer with regard to the following principles of confidentiality, accuracy, relevance and utilisation in the use of personal information.

The most important piece of legislation in regards to cloud computing is the "Uniting and Strengthening America by Providing Appropriate Tools Required to Intersect and Obstruct Terrorism Act 2001" (the US Patriot Act") which in its most basic application requires any data holder to allow access to the federal government to any information held by that organisation in the United States. This Act has profound implications as many cloud computing platforms and applications used on tablets and mobile technologies are supported by cloud computing facilities situated in the USA and this Act obligates these platforms to allow access to the sensitive information they might hold (Heyink 2012). Chapter 9 of the Bill is dedicated to cross border information flows.

The impact of this foreign legislation influenced the South African Bill as it is based on these foreign acts, but it also places in increased compliance burden on users of the cloud computing environment as compliance with the local Bill will have to be supplemented with knowledge of where your service provider is housing the data centre and the legal requirements in that country.

The principle identified regarding different legislation in different countries and legislative jurisdictions is that processing and storage of data in a cloud can be performed if the country/ legislative jurisdiction have similar or stricter laws than the country the data subject is resident in and the data was gathered assuming there is no adverse legislative requirements in those foreign countries.

How the "strictness" of legislation would be measured is a legal question and beyond the scope of this study but it does allow the possibility to move data into the cloud on the premise and assurance that the laws governing the cloud service provider is more stringent and will thus result in more protection for the data subject than what the data subject would have had in the country of origin.

To understand and explore the requirements of the Bill some of the definitions of the Bill have to be explored as their meaning is integral in understanding the requirements and responsibilities that the Bill assigns the different parties in the date gathering and processing process.

4.1.2) Important POPI Bill Definitions

The following definitions form part of Chapter 1 of the Bill (Protection of Personal Information Bill, 2009):

Table 4.1 – POPI Definitions

Words defined in POPI Bill	Definition
"personal information"	means information relating to an identifiable, living, natural person, and where it is applicable, an identifiable, existing juristic person, including, but not limited to— *(a)* information relating to the race, gender, sex, pregnancy, marital status, national, ethnic or social origin, colour, sexual orientation, age, physical or mental health, well-being, disability, religion, conscience, belief, culture, language and birth of the person; *(b)* information relating to the education or the medical, financial, criminal or employment history of the person; *(c)* any identifying number, symbol, e-mail address, physical address, telephone number or other particular assignment to the person; *(d)* the blood type or any other biometric information of the person; *(e)* the personal opinions, views or preferences of the person; *(f)* correspondence sent by the person that is implicitly or explicitly of a private or confidential nature or further correspondence that would reveal the contents of the original correspondence; *(g)* the views or opinions of another individual about the person; and *(h)* the name of the person if it appears with other personal information relating to the person or if the disclosure of the name itself would reveal information about the person;
"operator"	means a person who processes personal information for a responsible party in terms of a contract or mandate, without coming under direct authority of that party;
"record"	means any recorded information- (a) regardless of form or medium, including any of the following: (1) Writing on any material; (2) information produced, recorded or stored by means of any tape-recorder, computer equipment, whether hardware or software or both, or other device, and any material subsequently derived from information so produced, recorded or stored; (3) label, marking or other writing that identifies or describes anything of which it forms part, or to which it is attached by any means; (4) book, map, plan, graph or drawing;

Words defined in POPI Bill	Definition
	(5) photograph, film, negative, tape or other device in which one or more visual images are embodied so as to be capable, with or without the aid of some other equipment, of being reproduced; (b) in the possession or under control of a responsible party; (c) Whether or not it was created by a responsible party; and (d) regardless of when it came into existence;
"responsible party"	means a public or private body or any other person which , alone or in conjunction with others, determines the purpose of and means for processing personal information;
"processing"	means any operation or activity or any set of operations, whether or not by automatic means, concerning personal information, including- (a) the collection, receipt, recording, organisation, collation, storage, updating or modification, retrieval, alteration, consultation or use; (b) dissemination by means of transmission, distribution or making available in any other form; or (c) merging, linking, as well as restriction, degradation, erasure or destruction of information;
"account number"	for the purposes of section 105 (refer 4.3.1) means any unique identifier that has been assigned- (a) to one data subject only; or (b) jointly to more than one data subject, by a financial or other institution which enables the data subject, referred to in paragraph (a), to access his, her or its own funds or to access credit facilities or which enables a data subject, referred to in paragraph (b), to access joint funds or to access joint credit facilities.

Source: Compiled from the Protection of Personal Information Bill, 2009

In terms of this study the "operator" as defined and the Cloud Service Provider (CSP) are the same party responsible for data processing and data storage in the cloud.

The Bill sets out eight conditions that are closely aligned with the international principles of data protection. In the table below these principles are discussed with the relevant implications on the responsible party (RP) and the cloud service provider (CSP).

Table 4.2 – Summary of POPI Bill Principles

Principle/ "Condition"	Discussion	Impact on Responsible Party	Impact on Cloud Service Provider
Accountability	The responsible party must ensure that the principles contained in the POPI Bill and all the measures that give effect to the principles are complied with.	The onus is on the responsible party (RP) to ensure accountability.	No direct effect on the cloud service provider (CSP), but the responsible party will require that the SLA between the two parties confirms that the CSP complies with the requirements of the Bill.
Processing Limitation	Personal information may only be processed in a fair and lawful manner with the consent of the individual.	The responsible party needs to obtain consent of the data subject to process information. Personal Information may only be collected directly from the data subject.	The cloud service provider will receive information from the responsible party but will have no responsibility that the requirements of the Bill are adhered to.
Purpose Specification	Personal information may only be processed for specific, explicit defined and legitimate reasons.	The responsibility party can only collect data for a specific purpose and the data subject has to be aware of the purpose.	The CSP has to ensure that records are not retained for longer than necessary and has to guard against processing data that is not in line with the original purpose.
Further processing limitation	Personal information may not be processed for a second purpose unless that processing is compatible or supplementary to the original purpose.	The RP has to ensure that no further processing of the data takes place that is not in line with its original purpose of collection. As the processing will primarily take place in the cloud the SLA will have to specify which data is collected for which purchase.	The CSP processing will be governed by the SLA with the RP.
Information Quality	Responsible parties must ensure that personal information is kept reliable, accurate and up-to-date.	The RP has to take reasonable steps to ensure personal information is complete, accurate, not misleading and updated where necessary.	The CSP cloud security and data integrity controls will have to be scrutinised by the RP. For a data subject to be able to update personal information there has to be a link from the web interface where information is gathered by the RP to the cloud to allow information to be corrected.
Openness	Regulator and the data subject to be aware that personal information is being collected by the responsible party.	The RP must maintain the documentation of all processing operations under its responsibility in terms of section 14 of the Bill or section 51 of the Promotion of Access to Information Act (17).	The onus to inform the data subject of collection rest with the RP and the CSP will not be impacted by this requirement. Section 18(1) (g) requires that the RP informs the data subject of the

Principle/ "Condition"	Discussion	Impact on Responsible Party	Impact on Cloud Service Provider
		The RP has to notify the data subject that personal information is being collected and where the source of the information is a third party inform the data subject of the source it is being collected from.	fact that the RP intends to transfer the information to another country or international organisation and the level of protection of personal information afforded by that country or international organisation.
Security Safeguards	Personal information must be kept secure against risk of loss, unauthorised access, interference, modification, destruction or disclosure.	See responsible party responsibilities in Section 4.2 of this chapter.	See Cloud Service Provider responsibilities in Section 4.3 of this chapter.
Data subject participation	Data subjects may request the correction or deletion of any personal information held about them that may be inaccurate, misleading or outdated.	The RP has to allow a data subject access to his/her personal information. The RP must create an application or system whereby a data subject can access data in the cloud and correct it.	The CSP has to secure the interface with the application or system. Due to the fact that personal information could be processed in the cloud of thousands of data subjects the verification and granting of access will be complex and will result in additional costs to the CSP and RP.

Source: Compiled from the Protection of Personal Information Bill, 2009

For data to be lawfully processed all eight conditions as set out by Bill has to be met.

The onus is on the responsible party to ensure that all the conditions in the Bill is met, and this can only be done by adhering to the requirements when gathering data and transferring data to and from the cloud. The cloud service provider has to manage the data security and integrity requirements when data is received, stored, processed and transferred.

The responsibilities placed on each party are clear and the apparent solutions to these responsibilities will now be explored. The discussions below will be based on the premise that the responsible party is making use of a cloud service provider to store and process sensitive data.

4.2) Impact on Responsible Parties

The responsibility of the responsible party is well defined in the Bill and to discharge the obligations as set out in the Bill the principles has to be complied with.

The impact on the Responsible party is twofold in that data processing and collection has to be secure in the local network (responsible party's network) and transmission between the cloud and the local network has to be secure.

The requirements are primarily situated in section 19 to 22 and are grouped under the "Security Safeguards" condition of the Bill (Heyink, 2012).

The discussion will comprise of the stating of the requirement as it is in the Bill followed by possible solutions as to how a responsible party could discharge the requirements of the Bill.

The first requirement is regarding security measures to ensure information integrity.

Section 19 of the Bill states:

Section 19: *(1) A responsible party must secure the integrity and confidentiality of personal information in its possession or under its control by taking appropriate, reasonable technical and organisational measures to prevent-*

(a) loss of, damage to or unauthorised destruction of personal information; and

(b) Unlawful access to or processing of personal information

(c) Regularly verify that the safeguards are effectively implemented; and

(d) ensure that the safeguards are continually updated in response to new risks or deficiencies in previously implemented safeguards.

(2) In order to give effect to subsection (1), the responsible party must take reasonable measures to-

(a) identify all reasonable foreseeable internal and external risks to personal information in its possession or under its control;

(b) Establish and maintain appropriate safeguards against the risk identified;

(3) The responsible party must have due regard to generally accepted information security practices and procedures which may apply to it generally or be required in terms of specific industry or professional rules and regulations.

In the cloud computing environment a major portion of the implications of section 19 will be outsourced to the cloud service provider, but in terms of Section 21 the responsibility is with the responsible party to enter into a "written contract" which ensures the responsible party that the required security measures are established and maintained.

These legal complexities of these contractual agreements are outside of the scope of this work and focus will be limited to the minimum requirements that a responsible party has to confirm in writing to manage the responsibility assigned by the Bill.

4.2.1) Service Level Agreements with Cloud Providers

The Service Level Agreement between a responsible party and a cloud service provider is one of the most important defences a responsible party has in limiting the risk assigned to the responsible party by the Bill. This is "written contract "is specifically required by Section 21 (1) and the responsible party has to monitor that the operator (CSP) establishes and maintains the security measures agreed to.

Section 21 of the Act states:

Section 21	*(1) A responsible party must, in terms of a written contract between the responsible party and the operator, ensure that the operator which processes personal information for the responsible party establishes and maintains the security measures referred to in section 19.* *(2) The operator must notify the responsible party immediately where there are reasonable grounds to believe that the personal information of a data subject has been accessed or acquired by any unauthorised person.*

Due to the different cloud computing models and the various different parties that may provide the cloud infrastructure and/or a platform as a service or software as a service the list of requirements are not exhaustive and focus is on the general principles that need to be addressed following from the requirements of the Bill.

The following should be addressed in the contract between the cloud service provider and the responsible party. (Heyink, 2012)

- Any confidentiality requirements that the responsible party has agreed to with the data subject. This will be based on the data the responsible party has designated as sensitive;
- Records management. The format records and process results are held, retrieving protocols and any possible legal requirements on the responsible party. The legal admissibility of documents could depend on the format and security under which it is held;
- Record destruction and retention. The terms will have to be agreed between the two contracting parties as to the periods that document back-ups should be kept, the notice period given to the cloud provider when a document or data needs to be retrieved out of the data archives and the period that back-ups will be held by the cloud service provider;
- Sub-contractors will need to be identified and the same processing and confidentiality assurances need to be agreed upon that is applicable to the principle cloud service provider;
- Verification and audit of agreed upon security processes will need to be captured in the contract as the responsibility to ensure that there are proper security protocols and that that are implemented and maintained rests with the responsible party;
- Service levels have to be agreed between the contracting parties for example (up-time, server response time, and cost per measurable unit);
- A review of the Business Continuity and Disaster Recovery plans (DRP) of both the Cloud provider and the sub-contractor has to be done as well as confirming how a major event will impact on the responsible parties business. Regular tests and simulations of the "switch over" moment have to be done to confirm an active DRP.

The only method available to the responsible party to obtain the required assurance that the cloud provider has implemented and is maintaining the agreed/required level of security controls is to obtain independent assurance.

4.2.2) Assurance Reports

In order to discharge the responsibilities of the responsible party in terms of the Bill the responsible party can make use of the SAS 70/ISAE 3402 Auditing Standard regarding Assurance Reports on Controls at a Service Organization. The Standard supplies an independent review of controls, either enhancing a cloud provider's credibility or highlighting potential inadequacies (NDB Accountants & Consultants, 2008).

In terms of ISAE (International Standards on Assurance Engagements) the assurance provider can either receive a Type I or Type II report. Type I refers to assurance over the design and implementation of controls and the Type II report provides assurance over the effective operation of controls for a defined period (NDB Accountants & Consultants, 2008).

The assurance report can provide the required assurance to discharge the requirement set out in section 20 of the Bill.

The Bill places the responsibility on the responsible party to secure the integrity and confidentiality of personal information by taking appropriate, reasonable technical and organisational measures to prevent data loss or manipulation (POPI, 2009).

When the processing and/or storage of data is outsourced to an operator (CSP) the responsibility is still with the responsible party and the only remedy available is to discharge his responsibilities by using an appropriate SLA and confirming independently that the appropriate controls are implemented and maintained by the operator (CSP).

Due to the fact that most of the cloud service providers are based outside the South African borders an additional legislative requirement has to be addressed. Chapter 9 is focused on Trans-Border Information Flow and particular the provision that a responsible party cannot transfer personal information about a data subject to a third party outside the Republic unless there is a binding agreement and the foreign country upholds the principles of lawful processing.

4.2.3) Trans-border Information Flows

Chapter 9 of the Bill deals with trans-border information flows.

Section 72 (1) reads as follows:

Section 72 (1) A responsible party in the Republic may not transfer personal information about a data subject to a third party who is a foreign country unless-

(a) the third party who is the recipient of the information is subject to a law, binding corporate rules, binding agreement or memorandum of understanding entered into between two or more public bodies, which provide an adequate level of protection that-

(i) Effectively upholds principles for reasonable processing of the information that are substantially similar to the conditions for the lawful processing of personal information relating to a data subject who is a natural person and, where applicable, a juristic person; and

(ii) includes provisions, that are substantially similar to this section, relating to the further transfer of personal information from the recipient to third parties who are in a foreign country;

(b) the data subject consents to the transfer;

(c) the transfer is necessary for the performance of a contract between the data subject and the responsible party, or for the implementation of pre-contractual measures taken in response to the data subject's request;

(d) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the responsible party and the a third party; or

(e) the transfer is for the benefit of the data subject , and-

(i) it is not reasonably practicable to obtain the consent of the data subject to that transfer; and

(ii) if it were reasonably practicable to obtain such consent, the data subject would be likely to give it.

Section 72 (2) Where the transfer of personal information, as referred to in subsection (1), is made in terms of a non-binding memorandum of understanding the public body remains accountable for the purposes of this Act for the protection of the personal information.

*Section 72 (3) has a definition for **"accountable"** as it is used in section (2) above:*

***"accountable"** means that where the recipient of the information , who is a party to a non-binding memorandum of understanding, processes the personal information of a data subject in a manner that would have constituted an interference with the privacy of the data subject in terms of this Act had the information been processed in the Republic, the processing will be regarded as an interference with the privacy of the data subject in terms of this Act and will be regarded as having been processed by the responsible party.*

The legislative requirement that flows from this section is the requirement that a data subject has to give consent for their data to be transferred across borders. This consent will need to be obtained at the point where data is gathered. This requires the responsible party to plan into the future and amend the current data gathering processes to include this permission requirement.

The second requirement that flows out of this part of the Bill is that the local legislative requirement of the country where the operator (CSP) is situated has to be on the same standard as the promulgated POPI Bill. This is a technical legal requirement and an expert needs to be contacted to either confirm or disprove the level of legislation. It is unlikely that a CSP can give any assurance in this regard.

4.2.4) Obtaining permission

The responsible party will have to obtain the consent of the data subject to comply with the second condition of "Processing Limitation". The Bill does not however require that the consent of the data subject to be in writing. This result in processing being lawful if that data subject had the opportunity to object to the use of his/her personal information and fails to do so. In legal terms consent may be inferred (Heyink, 2011).

4.2.5) Securing data being transferred to and from the cloud

Based on the study into technical data security field in Chapter 3 the responsible party will have to secure the local network as well as all gateways in and out of the home network to the cloud.

The responsible party will have to implement an Information Security Framework with the appropriate level of Cloud Governance as well as technical security solutions to secure the different infrastructure in the network.

Due to the different configurations that can be used to build the interface with the cloud environment the securitisation of the data is fairly complex. Based on the cloud infrastructure and the service models that the responsible party a combination of solutions discussed in Chapter 3 can be implemented.

As an example: If the responsible party uses the SAAS service model and data is thus gathered from the data subject and passed into the cloud via a web browser the security available to secure the data gathering (web-browser security) as well as encryption and data storage controls has to be implemented. These will be addressed by the CSP and not the responsible party.

If the responsible party uses only the IAAS service model the responsible party will need to secure the data gathering by implementing control over the gathering of data as well as additional controls at the gateways into the cloud from the local network.

Based on the deployment model and the services that the responsible party wants to commit into the cloud environment the data security controls will have to be aligned with the risk associated with the model followed.

4.3) Impact on Cloud Service Providers

The various legislative requirements around the world regarding data storage and data processing have created a layer of complexity to most cloud service providers. 58 countries have National data privacy legislation governing the use of personal information (Imperva, 2013). Most developed countries has some form of juristic requirement on where data is stored as well as having requirements as to the controls and safeguards that is required before the service provider can receive data.

The POPI Bill places the onus on the responsible party to implement the eight principles as well as sections 19 to 21 regarding security measures but as the cloud service provider might be entity doing the storing and processing of the sensitive data the responsibility resides with the cloud provider to implement and maintain the necessary safeguards and processes to discharge these requirements.

4.3.1) Information processed by operator or person acting under authority – Section 20

Section 20 of the Bill states:

> *Section 20 An operator or anyone processing personal information on behalf of a responsible party or an operator, must-*
>
> *(a) process such information only with the knowledge or authorisation of the responsible party; and*
>
> *(b) treat personal information which comes to their knowledge as confidential and not disclose it,*
>
> *unless required by law or in the course of the proper performance of their duties.*

The CSP will have to perform only the processing that is required in terms of the service level agreement discussed in 4.2.1. The responsibility to comply with this section can be implemented by through access into the cloud through a web browser.

The complexity will however be due to the requirement that data in the cloud be partitioned (See 3.1 – Multi-Tenancy Model) and with numerous users needing access a strong controls over the virtualization of servers (See section 3.4.3) the CSP will have to implement strong controls over access.

Ryan (2013) comments that the cloud environment is not different from a normal network environment as data is always vulnerable irrespective of where it is stored and there are numerous ways to secure this data storage and processing, but cloud computing brings the additional risk that data can be accessed by the cloud provider, his sub-contractors and employees.

Ryan (2013) further discusses four possible ways to secure the data from access by the CSP. Possible solutions are to use fully homomorphic encryption (See 3.4.2), Key translator in the browser (See 3.4.5), Hardware-Anchored security (see 3.4.6) using the trusted platform module hardware chip and CryptDB.

CryptDb has not been discussed in this study as it is a form of SQL queries that uses encryption keys to access encrypted data decrypt the data and return the correct data required by the query. Encryption has been discussed in 3.4.2.

4.3.2) Security measures regarding information processed by an operator – Section 21

The Bill defines the responsibility clearly for operators/cloud service providers. The cloud service provider has to perform the following actions to comply with section 21 (1).

Section 21 of the POPI Bill requires the following:

> *Section 21 (1) A responsible party must, in terms of a written contract between the responsible party and the operator, ensure that the operator which processes personal information for the responsible party establishes and maintains the security measures referred to in section 19.*
>
> *(2) The operator must notify the responsible party immediately where there are reasonable grounds to believe that the personal information of a data subject has been accessed or acquired by any unauthorised person.*

In order for the operator/cloud service provider to discharge the obligations imposed by the bill a structured process has to be followed.

The first steps are to implement an information security framework (see 3.2) and the appropriate cloud governance structures that support the framework (see 3.3).

To manage the technical side of the requirements of section 21 (1), Imperva (2013) submits that an additional six steps has to be followed to allow the operator/CSP to manage the obligation. Step five and six both refer to monitoring access and alerting the appropriate parties the two steps has been combined and is discussed in intrusion detection.

The steps that Imperva proposes are set out below:

Step 1) Identify all PPI (Personal Identifiable Information) and Sensitive data

A cloud service provider needs to identify all PPI and sensitive data stored in the cloud. PPI data cannot be managed, monitored or safeguarded unless all locations where sensitive data is stored across the cloud network are identified.

As PPI data might be moved by users IP addresses and host names needs to be recorded and the cloud will have to be continually scanned for similar PPI and other sensitive data.

Step 2) Find, analyse and correct database vulnerabilities

Cloud service providers need to implement a thorough data risk management process that needs to be on-going. The cloud service provider can use database vulnerability assessment tools such as DISA STIG (Defence Information Systems Agency Security Technical Implementation Guides) or CIS benchmarks (Centre for Internet Security).

The DISA STIG publications contain technical guidance on how to protect information systems and software products and the CIS Benchmarks are consensus based, best practice security configuration guidelines both developed and accepted by government, business, industry and academia.

Any vulnerability identified needs to rank according to their severity. The Common Vulnerability Scoring System (CVSS) can be used and risk can be measured and weighted accordingly.

Step 3) Identify users that has access to Private Information

Sensitive data in the cloud can be stored and processed amongst numinous databases and to identify all user rights and privileges can be a complex task for the cloud service provider.

The cloud service provider has to aggregate access rights and store these in a single repository. Actively manage (review rights for appropriateness) the access rights of dormant users and restrict the rights of active users to sensitive information.

Step 4) Protect data from Unauthorised Access

Imperva refers to encryption and the masking of sensitive data but the securing of the cloud has been discussed and investigated in detail in Chapter 3 and there are numerous methods of obtaining the required security as well as measuring its effectiveness.

Step 5) Detect data base intrusions

Cloud Service provider has to implement an Intrusion Detection System (IDS) or preferably an Intrusion Detection and Prevention System (IDPS) (see section 3.4.5)

The requirement legislated in section 22(1) regarding the notification of the data subject if PPI information has been accessed will be addressed by the IDS or the IDPS. The notification will not be performed by the IDS system, but the CSP will be informed of a breach and notification process will be instigated from the alarm raised by the IDS. If the Cloud Provider can prevent access this is preferable due to both the civil responsibility that might arise from the unauthorised use of a data subject's information and the reputational and trust damage that will be incurred if there is a large amount of data compromised.

Section 22 of the Bill states (only applicable sections noted):

Section 22	*(1) Where there are reasonable grounds to believe that the personal information of a data subject has been accessed or acquired by any unauthorised person, the responsible party must notify –* *(a) The Regulator; and* *(b) subject to subsection (3), the data subject, unless the identity of such data subject cannot be established* *(3) The Responsible party may only delay notification of the data subject if a public body responsible for the prevention, detection or investigation of offences or the Regulator determines that notification will impede a criminal investigation by the public body concerned.*

If a data base intrusion is detected and not contained the bill requires explicit disclosure to the data subject. This can either be in the form of a letter, e-mail or on the website of the responsible party or published in the news media. (POPI, 2009)

Chapter 6 of the Bill requires that a party must notify the Regulator prior to processing and as the majority of processing in the cloud will be automated this requirement is problematic and will require the CSP to implement additional processes to comply with this requirement.

4.3.3) Notification

Chapter 6 (Sections 50 to 54) of the Bill is especially onerous.

Section 50 requires that a responsible party must notify the Regulator before commencing the-

(a) fully or partly automated processing of personal information or categories of personal information intended to serve a single purpose or different related purposes; and

(b) non-automated processing of personal information intended to serve a single purpose or different related purposes, must be notified if this is subject to a prior investigation.

The notification referred to above must be noted in a register kept by the Regulator for this purpose.

Section 51 requires that the notification must contain the following particulars:

(a) The name and address of the responsible party;

(b) the purpose of the processing

(c) a description of the categories of data subjects and of the information or categories of information relating thereto;

(d) the recipients or categories of recipients to whom the personal information may be supplied;

(e) planned transborder flows of personal information; and

(f) a general description allowing a preliminary assessment of the suitability of the information security measures to be implemented by the responsible party to ensure the confidentiality, integrity and availability of the information which is to be processed.

This section requires that the responsible party must notify the individual whose personal information is being processed at the time of collection regarding the purpose of collection and the parties to whom the personal information will be disclosed. If the personal information is collected directly from the individual, then the notification must take place before the collection.

This is practically difficult for a business as businesses evolve and the uses and third parties that might be exposed to the information changes over time. To inform the individual at the source of all of the possible uses and parties involved will hinder that gathering of information due to more time required to complete the process as well as placing a administrative burden on the business gathering the information.

If information is not gathered form an individual the business must ensure that the notification takes place as soon as reasonably practical after the collection of the personal information.

Additional to the notification of the data subject the Regulator must also be notified of the processing as required in section 51. This will require that controls be built into the processing system to inform the business and possibly the Regulator each instance where data is processed for a different reason than was previously

communicated. This could require a substantial investment in programming time to build the system that passes this detail to the Regulator.

The responsible party will only have to give notice once and the notification does not have to be repeated every time information is processed or received, only when the purpose of the processing has changed.

Any processing which departs from that that which has been notified to the Regulator must be recorded and kept for at least three years.

4.4) Enforcement (Offences, Penalties and Administrative fines)

Chapter 11 of the Act deals with the enforcement and implications of the Act.

Selected sections of chapter 11 will be discussed below:

4.4.1) Offences and Penalties

The implications of the POPI Bill can only be studied in relation to the severity of the penalties that can be imposed if the requirements of the Bill are not adhered to. By legislating the requirements for processing and storing personal data the legislature has raised the risk from a purely reputational impact to that of possible incarceration.

The relevant sections of the Bill are discussed below:

Table 4.3 lists the sections of the Bill that may not be contravened and is punishable by a prison sentence up to 10 years. Table 4.4 lists additional sections that may not be contravened, but here the prison term is limited to a maximum of 12 months.

Section 107(a): Any person convicted of an offence in terms of this Act, is liable, in the case of a contravention of section-

Table 4.3 – Contravention of these sections will be penalised for 10 years imprisonment

Sections in the Bill that may not be contravened	Discussion of Section
100	Obstruction, hindering or unlawfully influences the Regulator or any person acting on behalf or under direction of the Regulator.
103(1)	Responsible party fails to comply with an enforcement notice (Issued in terms of section 95 instructing the responsible party to either take specific steps or refrain from taking specific steps or stop processing personal information specified in the notice.
104(2)	Any person after being sworn in or making an affirmation gives false evidence, knowing such evidence to be false or not knowing or believing it to be true, is guilty of an offence.
105(1)	A responsible party who contravenes the provisions of section 8 (responsible party to ensure lawful processing through 8 principles) insofar those provisions relate to the processing of an account number of a data subject.
106(1), (3),(4)	Unlawful acts by third parties in connection with an account number such as a person knowingly or recklessly, without the consent of the responsible party (1) obtains or discloses an account number, selling an account number (3) which was unlawfully obtained or offering to sell an account number unlawfully obtained (4).

Source: Compiled from the POPI Bill, 2009

Contravention will result in the following:

*A fine or imprisonment for a period not exceeding **10 years** or both a fine and such imprisonment; or*

Section (b)-

Table 4.4 - Contravention of these sections will be penalised for 12 months imprisonment

Sections in the Bill that may not be contravened	Discussion of Section
59	In terms of section 57 and 58 the Regulator has to be informed if a responsible party plans to do any processing for another purpose than the one which the identifier was specifically intended at collection and with the aim of linking the information with information processed by other responsible parties. Section 59 deems it an offence if the disclosure was not done and the possible penalty is set out after the table.
101	Section 101 deems anybody that contravenes section 54 guilty of an offence. Section 54 requires that any person acting on behalf or under the direction of the Regulator must treat all personal information as confidential.
102	Obstructing a person in the execution of a warrant.
103(2)	Any responsible party that knowingly makes a false statement or recklessly make a material false statement in the compliance of an information notice in terms of section 90 (Notice from Regulator to responsible party requesting information on what processing is taking place)
104(1)	Any person failing without cause to attend legal proceeding based on a summons.

Source: Compiled from the POPI Bill, 2009

Contravention will result in the following:

*A fine or imprisonment for a period not exceeding **12 months** or both a fine and such imprisonment.*

The penalties imposed by the Bill are severe and punishable by ether prison sentences or administrative fines as can be seen below. These penalties are not trivial and will serve as a deterrent to responsible parties and operators (CSP) to comply with the legislative requirements.

4.4.2) Administrative Fines

Section 109 (2) (b) states that a notice will be given to the responsible party that will specify the alleged offence and section (c) requires that the amount of the fine must be specified, subject to chapter 11 section 10, but not exceeding R10 million.

Section 109 (2) (d) of the Bill states:

Section (d) The infringer may:

(i) pay the administrative fine;

(ii) make arrangements with the Regulator to pay the administrative fine in instalments;

(iii) elect to be tried in court on a charge of having committed the alleged offence referred to in terms of this Act.

If the Infringer elects (iii) above the case must be handed over to the South African Police Force and the infringer has to be informed accordingly.

Section 10 states that the Minister may after consultation with the Regulator adjust the amount of R10 million that is referred to in section 2 (c) by taking the consumer price index into account over the previous 12 months.

4.5) Conclusion

The signing by Parliament of the POPI Bill has raised the question regarding the impact of the Bill on businesses gathering, processing and storing personal information. The further complexity regarding cloud computing storage and processing has necessitated a study regarding the major effects of the Bill in relation to cloud computing users and providers.

The Bill places the onus to protect personal information on the responsible party regarding its gathering, processing and dissemination and if the responsible party uses a cloud service provider this responsibility is shared.

The Bill is also specific in its requirement regarding cross-border information flows and the penalties and fines that it proposes if contravened.

The study posed the question whether cloud computing was still a viable processing and storage method after the implementation of the Bill. This question was investigated in Chapter 4 by comparing the requirements of the Bill to the literature study of possible solutions performed in Chapter 3.

It can be concluded that some of the cost benefits that cloud computing promises will be negated by the additional legislative requirements that the Bill imposes. This conclusion is based on the premise that prior to the Bill businesses would have had some form of security controls regarding data gathering, processing and storage, but The Bill has now placed specific requirements on the responsible party and the CSP and these will require an increased level of data security controls. Additional to this the complexity of cross-border data flows and the requirements of the Bill will definitely require an increased level of legal involvement to provide assurance that a specific CSP can be used.

CSP's will also be impacted as the Bill was based on international legislation and in order to retain their clients they might have to enter into stringent SLA's and additional monitoring processes to discharge the shared responsibilities of the Bill.

There can be no doubt that the promulgated Bill will have an effect on the way that personal data is stored and processed in South Africa and where data is of such a sensitive nature cloud computing and its benefits might not be a viable solution when the risks are compared to the benefits.

Chapter 5 – Conclusion

Cloud computing is a new field in Internet computing that provides novel perspectives in internetworking technologies and raises issues in the architecture, design and implementation of existing networks and data centres (Pallis, 2010).

With a growing number of businesses investigating a move to the cloud computing paradigm due to the perceived cost benefits and unlimited resource availability the impact of this paradigm shift has to be compared with the growing trend of legislating the protection of personal information.

The benefits of cloud computing is evident and to understand the hype around cloud computing it is relevant to summarize them. The list is not exhaustive or complete.

- **Lower computer hardware costs.** No high-powered and high-priced computer is required to run cloud computing's web-based applications. Since applications run in the cloud, not on the desktop PC, your desktop PC doesn't need the processing power or hard disk space demanded by traditional desktop software. When you're using web-based applications, your PC can be less expensive, with a smaller hard disk, less memory, more efficient processor, and the like.
- **Improved performance.** Computers in a cloud computing system boot and run faster because they have fewer programs and processes loaded into memory.
- **Reduced software costs.** Most cloud computing applications, such as the Google Docs suite, are totally free. That's a lot better than paying $200+ for similar Microsoft Office software.
- **Instant software updates.** A Cloud computing system has the potential to ensure that the latest web-based updates happen automatically and are available the next time there is a connection to the cloud. When a web-based application is accessed, the latest version will be available without requiring paying for or downloading an upgrade.
- **Improved document format compatibility.** There are no format incompatibilities or limitations on documents created on one computer that is running a different version of the same software as all documents created by web-based applications can be read by any other user accessing that application.
- **Unlimited storage capacity.** Cloud computing offers virtually limitless storage.
- **Increased data reliability.** Due to the fact that data is stored in the cloud and the cloud service provider having more resources to secure and backup data the risk of data being corrupted is less than in a desktop environment.
- **Universal document access.** Documents are always available as long as there is a connection to the cloud. An example of this type of solution is DROPBOX.
- **Latest version availability.** Another document-related advantage of cloud computing is that all parties using a document or updating a document always as the current document available.
- **Device independence.** The User of the cloud computing paradigm is no longer constraint by a single computer or network. Computers and mobile devices are thin clients to the cloud and as long as there is an Internet connection available the user can move freely in his environment. Change computers, and your existing applications and documents follow you through the cloud.

To a business with limited resources cloud computing will seem like a solution to enable low cost, scalable processing where the user is only billed for the processing capacity used.

The type of business and the type of data that the business collects and processes will either confirm this premise or if the data is of a personal or sensitive nature it might result in a very expensive and complex system of processing and monitoring to the responsible party. Cloud computing relies heavily on the trust of third parties to implement the same stringent controls that a responsible party will have in their home network with the increased complicity of multiple users having access into the cloud.

This securing of the cloud is a daunting task and based on the study it would seem that even though the benefits noted above creates a very strong argument to move processing and data storage to the cloud the users and potential customers do not fully trust the paradigm (Bose, Luo, Lui, 2013) and (Circle ID Survey 2009).

This lack of trust is a central consideration for a business prior to moving into the cloud and with from a South African point of view these considerations became infinitely more important with the signing of the Protection of Personal Information Bill in August 2013.

In Chapter 2 the study investigated the impact of the new POPI Bill on cloud computing users by firstly investigating what technology constitutes cloud computing, its deployment and service models, and how it is defined. These studies resulted in a new cloud computing definition and based on this the data security controls that could be implemented to secure the defined cloud where investigated.

In Chapter 3 the requirements for secure data as it is legislated in the POPI Bill where used as a guideline in the investigation into the security themes that can be implemented to secure the cloud computing environment. The study focused on general themes and addressed each layer of the cloud computing environment and how to secure these layers. At a strategic level governance, risk management and information security frameworks where studied and at a data level encryption was investigated. Cloud computing uses virtualisation to store and process data and the controls that could be implemented where investigated. The interaction that users have with the cloud will normally take place through a web browser and the security that could be implemented where studied. The study concluded by looking at the methods to detect unauthorised access into the cloud as well as a hardware solution that when implemented will result in trusted computing between computers.

In Chapter 4 the detailed requirements and impact of the POPI Bill was investigated and the technology studied in Chapter 3 is mapped to the requirements of the Bill in figure 5.1.

The list of security measures are not exhaustive as the network design, deployment model used and service model might require additional security to discharge the requirements of the Bill.

The solutions are mapped based on the fact that either the responsible party or the cloud service provider or both has to address these requirements and based on the SLA between the parties the minimum requirements may differ.

Table 5.1 - Mapped security measures to POPI Bill requirements

Principle/ "Condition"	Discussion	Policy and procedure	Technical Data Security Measure
Accountability	The responsible party must ensure that the principles contained in the POPI Bill and all the measures that give effect to the principles are complied with.	• Information Security Framework • Cloud Governance and Risk Management processes • SLA	Technical measures to address accountability are addressed in the "Security Safeguards" section
Processing Limitation	Personal information may only be processed in a fair and lawful manner with the consent of the individual.	• Information Security Framework • Cloud Governance and Risk Management processes • SLA	• Virtualisation Monitoring • Cloud Intrusion Detection and Prevention
Purpose Specification	Personal information may only be processed for specific, explicit defined and legitimate reasons.	• Information Security Framework • Cloud Governance and Risk Management processes	• Virtualisation Monitoring • Cloud Intrusion Detection and Prevention • Web Service and Browser Security • Agreement with client regarding processing
Further processing limitation	Personal information may not be processed for a second purpose unless that processing is compatible or supplementary to the original purpose.	• Information Security Framework • Cloud Governance and Risk Management processes	• Agreement with client regarding processing
Information Quality	Responsible parties must ensure that personal information is kept reliable, accurate and up-to-date.	• Information Security Framework • Cloud Governance and Risk Management processes	• Virtualisation Monitoring • Cloud Intrusion Detection and Prevention • Web Service and Browser Security
Openness	Regulator and the data subject to be aware that personal information is being collected by the responsible party.	• Information Security Framework • Cloud Governance and Risk Management processes	• Agreement with client regarding processing • Cloud Intrusion Detection and Prevention

Principle/ "Condition"	Discussion	Policy and procedure	Technical Data Security Measure
			• Network transmission security
Security Safeguards	Personal information must be kept secure against risk of loss, unauthorised access, interference, modification, destruction or disclosure.	• Information Security Framework • Cloud Governance and Risk Management processes • Cloud risk identification processes	• Encryption • Virtualisation Monitoring • Web Service and Browser Security • Cloud Intrusion Detection and Prevention • Trusted Computing Module's
Data subject participation	Data subjects may request the correction or deletion of any personal information held about them that may be inaccurate, misleading or outdated.		• Web Service and Browser Security • Virtualisation Monitoring

The Protection of Personal Information Bill has set out the roadmap for responsible parties and cloud service providers to ensure lawful processing and secure data storage.

The principles of the Bill place the onus on the responsible party to comply and ensure lawful processing and if the processing and data storing are performed in the confines of a local network the responsible party will have control over the data security.

If the storage and processing is however performed in the cloud the only recourse to the responsible party is to consolidate the requirements of the Bill into a Service level agreement and to obtain independent assurance of the implementation and continued working of the cloud service provider data security controls.

Due to the complexity of cloud computing with numerous access nodes securing the cloud is a technical challenge and the fact that numerous users with unique access details might be required to interact with the cloud will result in complex access controls.

Information is an asset, like any other critical business asset and thus should be suitably protected. Businesses are increasingly interconnected which results in information being exposed to a growing number of threats and vulnerabilities. The move to legislate as in effect re-valued the information asset and as the process limitations and cross border data movement constraints are enforced the value of information will increase steadily.

Implementing cloud computing can provide businesses with an edge through cost savings but before embarking on the cloud computing path a thorough investigation needs to be performed by the responsible party regarding the type and sensitivity of that data that will be exposed to the cloud and with the POPI Bill and the Patriot Act placing onerous legislative requirements on cloud parties the cost savings might just be negated by legislative burden.

The International Organization for Standardization (ISO) standard setting body is currently completing ISO/IEC 27018 – Code of practice for data protection controls for public cloud computing services and this might assist to formalize the requirements regarding data protection.

The legal implications of the POPI Bill have not been tested and further study based on future case law and interpretations will be warranted.

References:

Amazon, *Amazon Elastic Compute Cloud (EC2)*, 2010, Viewed May 2013, Available at http://www.amazon.com/ec2/

Armbrust, M., Fox, A., Griffith, R., Joseph, A.D., Katz, R., Konwinski, A., Lee, G., Patterson, D., Rabkin, A., Stoica, I., Zaharia, M., 2009, Above the Clouds: A Berkeley View of Cloud Computing, Technical Report No. UCB/EECS-2009-28 viewed June 2011, http://www.eecs.berkeley.edu/Pubs/TechRpts/2009/EECS-2009-28.html

Brodkin, J., 2008, Gartner: Seven cloud-computing security risks, Gartner, Accessed July 2012, Available at www.idi.ntnu.no/emner/tdt60/papers/Cloud_Computing_Security_Risk.pdf

Bose, R., Luo, X.(Robert), Lui., 2013, The Roles of Security and Trust: Comparing Cloud Computing and Banking, The 2nd International Conference on Integrated Information, *Procedia - Social and Behavioural Sciences 73, 30-34*, Accessed June 2013, Available at: www.sciencedirect.com/science/article/pii/s187704281300308X

Buyya, R., Yeo, C.S., Venugopal, S., Broberg, J., Brandic, I., 2008, Cloud computing and emerging IT platforms: Vision, hype, and reality for delivering computing as a 5th utility, Future Generation Computer Systems (2009), doi:10.1016/j.future.2008.12.001, Viewed September 2011

Che, J., Duan, Y., Zhang, T., Fan, J., 2011, Study on the security models and strategies of cloud computing, 2011 International Conference on Power Electronics and Engineering Application, *Procedia Engineering* 23, 586-593, Accessed June 2013, Available at: www.sciencedirect.com/science/article/pii/S187770581105394X

Chen, D. & Zhao, H., 2012, "Data Security and Privacy Protection Issues in Cloud Computing", 2012 International Conference on Computer Science and Electronics Engineering. Accessed May 2013, Available at xa.yimg.com/kq/groups/2584474/417972861/name/NDU-1.pdf

Chen, Y., Paxson, V., Katz, 2010, *What's New About Cloud Computing Security?*, Technical Report No. UCB/EECS-2010-5, Available at: http://www.eecs.berkeley.edu/Pubs/TechRpts/2010/EECS-2010-5.html

Christodorescu, M., Sailer, R., Schales, D.L., Sgandurra, D., Zamboni, D., 2009, Cloud Security is not (Just) Virtualisation Security, IBM T.J.Watson Research, IBM Zurich Research.

Circle ID, "Survey: Cloud Computing "No Hype", But Fear of Security and Control Slowing Adoption", Accessed October 2013, Available at: http://www.circleid.com/posts/20090226_cloud_computing_hype_security/

Cloud Security Alliance 2009, "Security Guidance for Critical Areas of Focus in Cloud Computing V2.1", *Cloud Security Alliance,* http://www.cloudsecurityalliance.org/guidance/csaguide.v2.1.pdf, Accessed August 2013.

Cloud Security Alliance 2011, "Security Guidance for Critical Areas of Focus in Cloud Computing V3", *Cloud Security Alliance,* https://www.downloads.cloudsecurityalliance.org/initiatives/guidence/csaguide.v3.0.pdf, Accessed September 2013.

Conrad, E., 1997, Advanced Encryption Standard, Viewed August 2013, Available at www.giac.org/cissp-papers/42.pdf

Cornish, J. 2013, "South Africa's Protection of Personal Information Bill: The Law of Unintended Consequences, Latham & Watkins Middle East & Africa Technology, IP and Sourcing Focus, Accessed September 2013

Da Veiga, A., Eloff, J.H.P., 2007, An Information Security Governance Framework, Information Systems Management, 24:4, pp. 361-372

Data Loss Prevention, SANS Institute InfoSec Reading Room, P. Kanagasingham, 2008, Accessed 12/10/2013, http://www.sans.org/reading-room/whitepaper/32883.pdf

Dhir. A, 2000, "Data encryption using DES/Triple-DES Functionality in Spartan-II FPGAs, Accessed 10/10/2013, Available at http://www.xilinx.com

Dokakis M. 2013, Protection of Personal Information Bill (POPI) – Changing Industries*, Accountancysa*, http:// www.accountancysa.org.za/resources/showitemarticle.asp?ArticleId=2249&Issue=1106

El-Khameesy, N., Rahman, H.A., 2012, "A Proposed Model for Enhancing Data Storage Security in Cloud Computing Systems", *Journal of Emerging Trends in Computing and Information Sciences*, vol. 3, no. 6, June 2012, pp. 970-974

Enslin, Z., 2012, "Cloud Computing: COBIT-mapped benefits, risks and controls for consumer enterprises, University of Stellenbosch

Federal Information Processing Standard Publication 197 (FIPS), 2001, Advanced Encryption Standard (AES), Accessed September 2013, Available at: *csrc.nist.gov/publications/fips/fips197/fips-197.pdf*

Foster, I., Zhao, Y., Raicu, I., Lu, S., 2008, Cloud Computing and Grid Computing 360-Degree Compared, Accessed September 2011, Available at http://arxiv.org/pdf/0901.0131.pdf

Garfinkel, S., 2011, "The Cloud Imperative", in MIT Technology Review, Viewed September 2012, from www.technologyreview.com/news/425623/the-cloud-imperative

Garfinkel, T., Rosenblum, M., 2005, When virtual is harder than real: Security challenges in virtual machine based computing environments, Proceedings of the 10th conference on Hot Topics in Operating Systems-Volume 10. p. 20.USENIX Association

Gartner IT Glossary, Gartner, viewed August 2011, Available at www.gartner.com/it-glossary/cloud-computing/

Gartner, 2011, CIO Agenda Findings, Accessed July 2011, Available at: http://gartner.com/technology/cio/cioagenda_findingd.jsp

Heyink, M., 2011, Protection of Personal Information Guidelines for Law Firms, Law Society of South Africa, Version 1, Accessed May 2013, Available at: http://www.lssa.org.za/upload/Protection%20of%20Personal%20Information%20Guideline%202011%20v1_0%20110517(1).pdf

Heyink, M., 2012, An Introduction to Cloud Computing: Legal Implications for South African Law Firms, Law Society of South Africa, Accessed May 2013, Available at: http://www.lssa.org.za/upload/LSSA%20Guidelines_Introduction%20to%20Cloud%20Computing%20-%20Legal%20Implications%202012.pdf

Heyink, M., 2013, Protection of Personal Information Guidelines for Law Firms, Law Society of South Africa, Version 3, Accesed October 2013, Available at: http://www.lssa.org.za/upload/Protection%20of%20Personal%20Information%20Guideline%202013v3%20final.pdf

Imperva, 2013, Data Protection Under POPI: 6 Step Data Privacy Protection Plan for the South African Protection of Personal Information (POPI) Bill, Accessed September 2013, Available at http://www.imperva.com/docs/WP_Data_Protection_Under_POPI.pdf

International Organisation for Standardization, 1989, ISO 7498-2:1989*, Information processing systems—Open Systems Interconnection—Basic Reference Model—Part 2: Security Architecture*, Switzerland, International Organisation for Standardization (ISO).

International Organisation for Standardization, 2000, ISO/IEC 17799:2000, *Information technology – code of practice for information security management,* Switzerland: International Organisation for Standardization (ISO)

International Organisation for Standardization, 2005, ISO 27001:2005*,Information technology – Security techniques – Information security management systems - Requirements* , Switzerland, International Organisation for Standardization (ISO).

Information Systems Audit and Control Association (ISACA), 2009, Cloud Computing: Business Benefits With Security, Governance and Assurance Perspectives, An ISAC Emerging Technology White Paper, October 2009, Illinois, USA

Information Systems Audit and Control Association (ISACA), 2011, *It Control Objectives for Cloud Computing: Controls and Assurance in the Cloud*, Illinois, USA

Jansen, W., Grance, T., 2011, "Guidelines on Security and Privacy in Public Cloud Computing", Special Publication 800-144, National Institute of Standards and Technology, Maryland, USA

Jensen, M., Schwenk, J., Gruschka, N. & Iacono, L.L. 2009, "On technical security issues in cloud computing", *CLOUD 2009 - 2009 IEEE International Conference on Cloud Computing*, pp. 109-116.

Jericho Formu, 2009, Cloud Cube Model: Selecting Cloud Formations for Secure Collaboration, Accessed September 2013, Available at http://www.opengroup.org/jericho/cloud_cube_model_v1.0.pdf

Karlof, C., Tygar, J.D., Wagner, D., Shankar, U., 2007 , Dynamic Pharming Attacks and Locked Same-origin Policies for Web Browsers, Viewed October 2013, Available at: www.cs.berkeley.edu/~daw/papers/pharming-ccs07.pdf

Leong, M.P., Cheung, O.Y.H., Tsoi, K.H., Leong, P.H.W., 2000, A Bit-serial Implementation of the International Data Encryption Algorithm IDEA, The Chinese University of Hong Kong, Accessed August 2013, Available at https://courses.cs.washington.edu/courses/cse590g/01sp/fccm00_idea1.pdf

Mackay, M., Baker, T., Al-Yasiri, A., 2012, Security-orientated cloud computing platform for critical infrastructures, *Computer Law & Security review 28*, pp. 679-686

Mell, P. & Grance, T. 2011, "The NIST definition of cloud computing", Special Publication 800-145, National Institute of Standards and Technology, Maryland, USA

Mishra, A., Mathur, A., Jain, S., Rathore, J.S., 2013, Cloud Computing Security*, International Journal on Recent and Innovation Trends in Computing and Communication*, Volume 1, Issue 1, PP. 36-39

Modi, C.N., Patel, D.R., Patel, A., Rajarajan, M., 2012, Integrated Signature Apriori based Network Intrusion Detection System (NIDS) in Cloud Computing), *Procedia Technology*, 6, pp 905-912

Mukherjee, B., Heberlein, L.T., Levitt, K.N., 1994, Network Intrusion Detection, *IEEE Network*, May/June 1994, pp. 26-41

NDB Accountants & Consultants, 2008, SAS 70 Primerl, Accessed September 2013, Available at , http://www.sas70.us.com/white-papers/introduction-to-the-auditing-standard.php

Northcutt, S., 2008 Security Laboratory: Cryptography in Business Series: Hash Functions, Accessed October 2013, Available at: www.sans.edu/reserach/security-labratory/article/hash-functions

Pallis, G. 2010, Cloud Computing, The New Frontier of Internet Computing, University of Cyprus, IEEE Computer Society, Accessed June 2013, Available at http://www.techrepublic.com/resource-library/whitepapers/cloud-computing-the-new-frontier-of-internet-computing/

Patel, A., Taghavi, M., Bakhtiyari, K., Júnior, J. C., 2013, An intrusion detection and prevention system in cloud computing: A systematic review, *Journal of Network and Computer Applications*, 36, pp. 25-41

Plummer, D.C., Smith, D.M., Bittman, T.J., Cearley, D.W., Cappuccio, D.J., Scott, D., Kumar, R. & Robertson, B. 2009, "Five refining attributes of public and private cloud computing", *Gartner*, Research report, 5 May 2009

PWC, 2011, The POPI Bill, The journey to implementation, Accessed May 2013, Available at http://www.cioafricasummit.com/media/whitepapers/2012/PwC.pdf

Ramgovind S, Eloff MM, Smith E, 2010 'The Management of Security in Cloud Computing', Accessed June 2013, Available at http://umkn-dsp01.unisa.ac.za/xmlui/bitstream/handle/10500/3883/ramgovind.pdf?sequence=1

Ranchal, R., Bhargava, B., Othmane, L.B., Lilien, L., Kim,A., Kang,M., 2012, An Approach for Preserving Privacy and Protecting Personally Identifiable Information in Cloud Computing, ResearchGate, Accessed September 2013, Available at http://www.researcgate.net/publication/228649245_An_Approach_for_Preserving_Privacy_and_Protecting_Personally_Identifiable_Information_in_Cloud_Computing

Ryan M.D., Cloud computing security: The scientific challenge, and survey of solutions, The Journal of Systems and Software (2013), http://dx.dio.org/10.1016/j.jss.2012.12.025

Scarfone, K., Mell, P, 2007,NIST Special Publication 800-94 Guide to Intrusion Detection and Prevention Systems (IDPS), Revised January 2012

Schultz, E., 2008, Rootkits: The Ultimate Malware Threat, Information Security Management Handbook, Sixth Edition, Volume 2, Accessed October 2013, Available at: www.infosectoday.com/Articles/Rootkits.htm

Sotto, L.J., Treacy, B.C., McLellan, M.L., 2010, Privacy and Data Security Risks in Cloud Computing, BNA Electronic Commerce & Law Report, Bureau of National Affairs, Accessed August 2013, Available at: www.hunton.com/files/Publication/4845e31f-63d8-4f9a-9a36-a074e4170225/Presentation/PublicationaAttachment/6f52b2fd-2973-48cc-9f23-c941f1e19358/Privacy-Data_Security_Risks_in_Cloud_Computing_2.10.pdf

South Africa, Department of Justice, 2009, Protection of Personal Information Bill (B9B-2009), Viewed February 2013, Available at: www.justice.gov.za/legislation/bills/B9-2009_ProtectionofPersonalInformation.pdf

Studnia, I., Alata, E., Deswarte, Y., Kaâniche, M., Nicomette, V., 2012, Survey of Security Problems in Cloud Computing Virtual Machines, http://hal.inria.fr/docs/00/76/12/06/PDF/cesar_paper71-version_publieI_e.pdf

Subashini, S., Kavitha, V., 2010, A survey on security issues in service models of cloud computing, Journal of Network and Computer Applications, 2010, doi:10.1016/j.jnca.2010.07.006

The Trusted Computing Group, 2011, Trusted platform module specification version 1.2. Accessed October 2013, Available at: http://www.trustedcomputinggroup.org/resources/tpm_main_spesification

Vaquero, L. M., Rodero-Meniro, L., Caceres, J. & Lindner, M. 2009, "A Break in the clouds: towards a cloud definition", *Communication Review,* vol.3 9, no. 1, pp. 50-55.

Wang, L., von Laszewski, 2008, Scientific Cloud Computing: Early Definition and Experience, Viewed August 2011, Available at: http://cyberaide.googlecode.com/svn/trunk/papers/08-cloud/vonLaszewski-08-cloud.pdf

Wisegeek, (2013), What are the Different Encryption Techniques?, Viewed September 2013, Available at: www.wisegeek.com/what-are-the-different-encryption-techniques.htm

Yu, S., Wang, C., Ren, K., Lou, W., 2010, “Achieving Secure, Scalable, and Fine-grained Data Access Control in Cloud Computing”, Accessed July 2013

Zhang, Q., Cheng, L., Boutaba, R., 2010, Cloud computing: state-of-the-art and research challenges, *Journal of Internet Services and Applications*, May 2010, Volume 1, Issue 1, pp. 7-18

Zizziz, D., Lekkas, D., 2012, Addressing cloud computing security risks, *Future Generation Computer Systems*,Volume 28, pp. 583-592